管理事件和警報

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager-918/events/concept_what_active_iq_platform_events_are.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

管理事件和警報 1
管理事件 1
在 Active IQ Unified Manager 中了解 Active IQ 平台事件 1
什麼是事件管理系統事件 1
了解 Active IQ Unified Manager 如何處理接收到的事件 5
在 Active IQ Unified Manager 中查看事件詳情 6
在 Active IQ Unified Manager 中檢視未指派的事件 7
在 Active IQ Unified Manager 中確認並解決事件 7
在 Active IQ Unified Manager 中將事件指派給特定使用者 8
在 Active IQ Unified Manager 中停用不需要的事件 9
使用 Active IQ Unified Manager 中的自動修復功能來解決問題 10
在 Active IQ Unified Manager 中啟用並停用 Active IQ 事件報告 10
在 Active IQ Unified Manager 中上傳新的 Active IQ 規則檔案 11
Active IQ Unified Manager 如何產生 Active IQ 平台事件 12
在 Active IQ Unified Manager 中解決 Active IQ 平台事件 12
在 Active IQ Unified Manager 中設定事件保留設定 13
什麼是 Unified Manager 維護所需時間 13
在 Active IQ Unified Manager 中管理主機系統資源事件 15
進一步了解事件 16
事件和嚴重性類型列表 20
事件視窗和對話方塊的描述 64
管理警報 76
了解 Active IQ Unified Manager 中的警示 76
Active IQ Unified Manager 警報電子郵件中包含的資訊 76
新增警示 77
在 Active IQ Unified Manager 中新增效能事件警報 80
在 Active IQ Unified Manager 中測試警報 80
停用 Active IQ Unified Manager 中已解決與已過時事件的警報 81
將災難恢復目的地 Volume 從 Active IQ Unified Manager 的警報產生中排除 81
在 Active IQ Unified Manager 中查看警報 82
在 Active IQ Unified Manager 中編輯警報 82
在 Active IQ Unified Manager 中刪除警報 82
警告視窗和對話方塊的說明 83
管理指令碼 88
在 Active IQ Unified Manager 中管理指令碼 88
Active IQ Unified Manager 中的指令碼如何與警報協同運作 89
在 Active IQ Unified Manager 中新增指令碼 90
在 Active IQ Unified Manager 中刪除指令碼 90
在 Active IQ Unified Manager 中執行測試指令碼 91

瞭解受支援的 Active IQ Unified Manager CLI 指令 91
指令碼視窗和對話方塊的說明 96

管理事件和警報

管理事件

在 **Active IQ Unified Manager** 中了解 **Active IQ** 平台事件

Unified Manager 可以顯示 Active IQ 平台發現的事件。這些事件是透過對 Unified Manager 監控的所有儲存設備系統所產生的 AutoSupport 訊息執行一組規則而建立的。

如需詳細資訊，請參閱 "Active IQ 平台事件是如何產生的"。

Unified Manager 會自動檢查是否有新的規則檔案，並且只有在有新規則時才下載新檔案。在沒有外部網路存取的站點中，您需要從 儲存設備管理 > 事件設定 > 上傳規則 手動上傳規則。

這些 Active IQ 事件與現有的 Unified Manager 事件不重疊，它們識別與系統組態、佈線、最佳實務做法和可用度問題相關的事件或風險。

如需啟用平台事件的詳細資訊，請參閱 "啟用 Active IQ 入口網站事件"。如需上傳規則檔案的詳細資訊，請參閱 "上傳新的 Active IQ 規則檔案"。

NetApp Active IQ 是一項基於雲端的服務，可提供預測分析和主動支援，以最佳化 NetApp 混合雲環境中的儲存系統運作。請參閱 "NetApp Active IQ"以取得更多資訊。

什麼是事件管理系統事件

了解 **Active IQ Unified Manager** 中的事件管理系統事件

事件管理系統 (EMS) 從 ONTAP 核心的不同部分收集事件資料，並提供事件轉發機制。這些 ONTAP 事件可以作為 EMS 事件在 Unified Manager 中進行報告。集中式監控和管理簡化了關鍵 EMS 事件的組態以及基於這些 EMS 事件的警報通知。

將叢集新增至 Unified Manager 時，Unified Manager 位址會被新增為叢集的通知目的地。叢集中一發生事件，就會立即報告 EMS 事件。

Unified Manager 中有兩種接收 EMS 事件的方法：

- 一定數量的重要 EMS 事件會自動回報。
- 您可以訂閱以接收個別 EMS 事件。

Unified Manager 產生的 EMS 事件的報告方式會因事件產生方法的不同而有所差異：

功能	自動 **EMS** 訊息	訂閱的 **EMS** 訊息
可用的 EMS 事件	EMS 事件子集	所有 EMS 事件
觸發時的 EMS 訊息名稱	Unified Manager 事件名稱（由 EMS 事件名稱轉換而來）	格式為「Error EMS received」的非特定訊息。詳細訊息提供實際 EMS 事件的點記法格式

功能	自動 **EMS** 訊息	訂閱的 **EMS** 訊息
收到的訊息	一旦發現叢集	在將每個必要的 EMS 事件新增至 Unified Manager 後，以及在接下來的 15 分鐘輪詢週期之後
事件生命週期	與其他 Unified Manager 事件相同：新建、已確認、已解決和過時狀態	叢集重新整理後，EMS 事件會在事件建立的 15 分鐘後失效
擷取 Unified Manager 停機期間的事件	是的，系統啟動時會與每個叢集通訊以取得遺失的事件	否
事件詳細資料	建議的修正行動直接從 ONTAP 匯入，以提供一致的解決方案	事件詳細資料頁面中未提供修正行動

部分新增的自動 EMS 事件屬於資訊性事件，用於指示先前的事件已解決。例如，「FlexGroup 成員空間狀態一切正常」資訊性事件表示「FlexGroup 成員空間存在問題」錯誤事件已解決。資訊性事件無法使用與其他事件嚴重性類別相同的事件生命週期來代管，但如果同一 Volume 再次收到「`Space Issues`」錯誤事件，則該事件將自動失效。

自動新增至 **Active IQ Unified Manager** 的 **EMS** 事件

以下 ONTAP EMS 事件會自動加入到 Unified Manager。當在 Unified Manager 監控的任何叢集上觸發時，將會產生這些事件。

在監控執行 ONTAP 9.5 或更高版本軟體的叢集時，可以使用下列 EMS 事件：

Unified Manager 事件名稱	**EMS** 事件名稱	受影響的資源	**Unified Manager** 嚴重性
彙總重新定位的雲端層存取被拒絕	arl.netra.ca.check.failed	彙總	錯誤
在儲存設備容錯移轉期間，彙總重新定位的雲端層存取被拒絕	gb.netra.ca.check.failed	彙總	錯誤
FabricPool 鏡像複製重新同步完成	wafl.ca.resync.complete	叢集	錯誤
FabricPool 空間幾乎已滿	fabricpool.nearly.full	叢集	錯誤
NVMe-oF 寬限期已開始	nvmf.graceperiod.start	叢集	警告
NVMe-oF 寬限期作用中	nvmf.graceperiod.active	叢集	警告
NVMe-oF 寬限期已過期	nvmf.graceperiod.expired	叢集	警告
LUN 已毀損	lun.destroy	LUN	資訊
AWS 雲端平台 MetaDataConnFail	cloud.aws.metadataConnFail	節點	錯誤
雲端 AWS IAMCredsExpired	cloud.aws.iamCredsExpired	節點	錯誤

Unified Manager 事件名稱	**EMS** 事件名稱	受影響的資源	**Unified Manager** 嚴重性
雲端 AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	節點	錯誤
雲端 AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	節點	錯誤
雲端 AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	節點	資訊
雲端 AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	節點	錯誤
雲端 AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	節點	錯誤
雲端層主機無法解析	objstore.host.unresolvable	節點	錯誤
雲端分層叢集間網路介面故障	objstore.interclusterlifDown	節點	錯誤
要求不符的雲端層簽章	osc.signatureMismatch	節點	錯誤
其中一個 NFSv4 集區已耗盡	Nblade.nfsV4PoolExhaust	節點	關鍵
QoS 監控記憶體容量已滿	qos.monitor.memory.maxed	節點	錯誤
QoS 監控記憶體容量減少	qos.monitor.memory.abated	節點	資訊
NVMeNS 毀損	NVMeNS.destroy	命名空間	資訊
NVMeNS 線上	NVMeNS.offline	命名空間	資訊
NVMeNS 離線	NVMeNS.online	命名空間	資訊
NVMeNS 空間不足	NVMeNS.out.of.space	命名空間	警告
同步複寫不同步	sms.status.out.of.sync	SnapMirror 關係	警告
同步複製已恢復	sms.status.in.sync	SnapMirror 關係	資訊
同步複製自動重新同步失敗	sms.resync.attempt.failed	SnapMirror 關係	錯誤
許多 CIFS 連線	Nblade.cifsManyAuths	SVM	錯誤
CIFS 連線數已超過上限	Nblade.cifsMaxOpenSameFile	SVM	錯誤
每個用戶的 CIFS 連線數已超過最大值	Nblade.cifsMaxSessPerUsrConn	SVM	錯誤
CIFS NetBIOS 名稱衝突	Nblade.cifsNbNameConflict	SVM	錯誤
嘗試連接不存在的 CIFS 共享	Nblade.cifsNoPrivShare	SVM	關鍵
CIFS 陰影複製作業失敗	cifs.shadowcopy.failure	SVM	錯誤

Unified Manager 事件名稱	**EMS** 事件名稱	受影響的資源	**Unified Manager** 嚴重性
AV 伺服器發現病毒	Nblade.vscanVirusDetected	SVM	錯誤
沒有用於病毒掃描的 AV 伺服器連線	Nblade.vscanNoScannerConn	SVM	關鍵
未註冊任何 AV 伺服器	Nblade.vscanNoRegdScanner	SVM	錯誤
無回應的 AV 伺服器連線	Nblade.vscanConnInactive	SVM	資訊
AV 伺服器過於繁忙，無法接受新的掃描要求	Nblade.vscanConnBackPressure	SVM	錯誤
未經授權的使用者嘗試存取防毒伺服器	Nblade.vscanBadUserPrivAccess	SVM	錯誤
FlexGroup 成分區段發生空間問題	flexgroup.constituents.have.space.issues	磁碟區	錯誤
FlexGroup 組成部分空間狀態全部正常	flexgroup.constituents.space.status.all.ok	磁碟區	資訊
FlexGroup 成員有 Inode 問題	flexgroup.constituents.have.inodes.issues	磁碟區	錯誤
FlexGroup 組成 Inode 狀態全部正常	flexgroup.constituents.inodes.status.all.ok	磁碟區	資訊
磁碟區邏輯空間幾乎已滿	monitor.vol.nearFull.inc.sav	磁碟區	警告
磁碟區邏輯空間已滿	monitor.vol.full.inc.sav	磁碟區	錯誤
Volume 邏輯空間正常	monitor.vol.one.ok.inc.sav	磁碟區	資訊
WAFL 磁碟區 AutoSize 故障	wafl.vol.autoSize.fail	磁碟區	錯誤
WAFL 磁碟區 AutoSize 已完成	wafl.vol.autoSize.done	磁碟區	資訊
WAFL READDIR 檔案操作逾時	wafl.readdir.expired	磁碟區	錯誤

在 **Active IQ Unified Manager** 中訂閱 **ONTAP EMS** 事件

您可以訂閱接收安裝了 ONTAP 軟體的系統所產生的事件管理系統 (EMS) 事件。部分 EMS 事件會自動回報給 Unified Manager，但其他 EMS 事件只有在您訂閱這些事件後才會回報。

開始之前

請勿訂閱已自動新增至 Unified Manager 的 EMS 事件，因為收到相同問題的兩個事件可能會導致混淆。

您可以訂閱任意數量的 EMS 事件。您訂閱的所有事件都會經過驗證，而且只有經過驗證的事件才會套用到您在 Unified Manager 中監控的叢集。*ONTAP 9 EMS* 事件目錄 提供指定 ONTAP 9 軟體版本的所有 EMS 訊息的詳

細資訊。從 ONTAP 9 產品文件頁面尋找適當版本的 *EMS* 事件目錄，以取得適用事件的清單。

"ONTAP 9 產品庫"

您可以為訂閱的 ONTAP EMS 事件設定警報，也可以建立針對這些事件執行的自訂指令碼。

如果您未收到已訂閱的 ONTAP EMS 事件，可能是叢集的 DNS 組態有問題，導致叢集無法連線至 Unified Manager 伺服器。若要解決此問題，叢集管理員必須修正叢集的 DNS 組態，然後重新啟動 Unified Manager。這樣做會將待處理的 EMS 事件傳送到 Unified Manager 伺服器。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 事件設定。
2. 在「事件設定」頁面中，點選 訂閱 **EMS** 事件 按鈕。
3. 在「訂閱 EMS 事件」對話方塊中，輸入要訂閱的 ONTAP EMS 事件的名稱。

   若要檢視您可以訂閱的 EMS 事件名稱，您可以從 ONTAP 叢集 shell 使用 `event route show`命令（ONTAP 9 之前）或 `event catalog show`命令（ONTAP 9 或更新版本）。

   "如何在 Active IQ Unified Manager 中設定和接收來自 ONTAP EMS 事件訂閱的警報"

4. 點擊 **Add** 。

   EMS 事件已新增至已訂閱的 EMS 事件清單中，但「適用於叢集」欄位顯示您新增的 EMS 事件的狀態為「`Unknown`」。

5. 按一下 儲存並關閉 以向叢集註冊 EMS 事件訂閱。
6. 再次點選 訂閱 **EMS** 事件。

   您新增的 EMS 事件的「適用於叢集」欄中會顯示狀態 “Yes”。

   如果狀態不是「`Yes`」，請檢查 ONTAP EMS 事件名稱的拼字。如果名稱輸入錯誤，您必須移除不正確的事件，然後再次新增該事件。

當 ONTAP EMS 事件發生時，該事件會顯示在「事件」頁面上。您可以選取事件，以在「事件詳細資料」頁面中檢視 EMS 事件的詳細資料。您也可以管理事件的處置方式，或為事件建立警示。

了解 **Active IQ Unified Manager** 如何處理接收到的事件

當 Unified Manager 收到事件時，它會顯示在儀表板頁面、事件管理清單頁面、叢集/效能頁面的摘要和資源管理器標籤，以及物件專屬的清單頁面（例如， Volume / 健全狀況清單頁面）中。

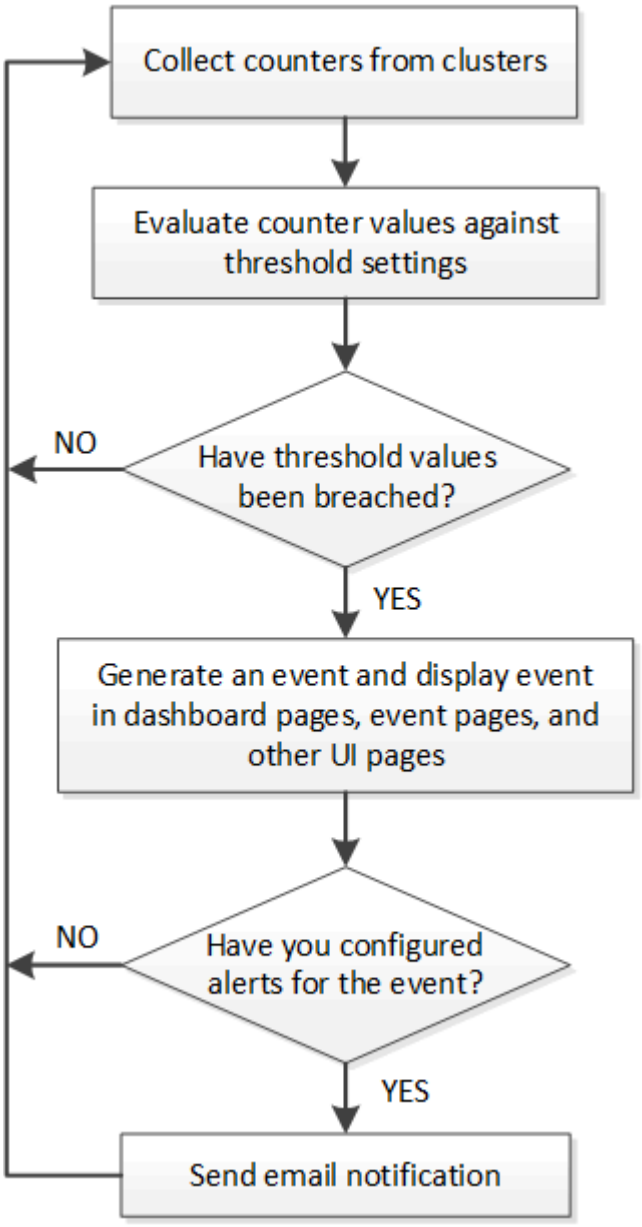
當 Unified Manager 偵測到相同叢集元件的相同事件條件多次連續發生時，它會將所有發生情況視為單一事件，而不是分隔的事件。事件的持續時間會遞增，以表示該事件仍在作用中。

根據您在「警報設定」頁面中的設定方式，您可以將這些事件通知其他使用者。警報會觸發以下行動：

- 可以向所有 Unified Manager 系統管理員使用者發送有關此事件的電子郵件。
- 該事件可以發送給其他電子郵件收件者。

- 可以將 SNMP 陷阱傳送到陷阱接收器。
- 可以執行自訂指令碼來執行行動。

此工作流程如下圖所示。



在 **Active IQ Unified Manager** 中查看事件詳情

您可以檢視由 Unified Manager 觸發之事件的詳細資訊，以便採取修正行動。例如，如果出現「Volume 離線」健全狀況事件，您可以按一下該事件以檢視詳細資訊並執行修正行動。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

事件詳情包括事件來源、事件起因以及與事件相關的任何備註等資訊。

步驟

1. 在左側導覽窗格中，按一下 事件管理。

   預設情況下，「所有作用中事件」檢視會顯示過去 7 天內產生的、影響等級為「事件」或「風險」的新事件和已確認（作用中）事件。

2. 如果您想檢視特定類別的事件，例如容量事件或效能事件，請按一下 檢視，然後從事件類型選單中進行選擇。
3. 按一下您要檢視詳細資料的事件名稱。

   事件詳細資料會顯示在事件詳細資料頁面中。

在 **Active IQ Unified Manager** 中檢視未指派的事件

您可以檢視未指派的事件，然後將每個事件指派給能夠解決該事件的使用者。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下 事件管理。

   預設情況下，新事件和已確認事件會顯示在事件管理清單頁面上。

2. 在 篩選器 窗格中，選取 指派給 區域中的 未指派 篩選選項。

在 **Active IQ Unified Manager** 中確認並解決事件

在著手處理引發該事件的問題之前，您應該先確認該事件，以免繼續收到重複的警報通知。針對特定事件採取修正行動後，您應該將該事件標記為已解決。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

您可以同時確認和解決多個事件。

您無法確認資訊事件。

步驟

1. 在左側導覽窗格中，按一下 事件管理。
2. 從事件清單中，執行以下操作以確認事件：

如果您想要.....	這樣做.....
確認並標記單一事件為已解決	a. 點選事件名稱。 b. 從事件詳細資料頁面中，判斷事件的原因。 c. 按一下 確認。 d. 採取適當的修正行動。 e. 按一下 標記為已解決。
確認並標記多個事件為已解決	a. 從相應的事件詳細資料頁面確定事件的原因。 b. 選擇事件。 c. 按一下 確認。 d. 採取適當的修正行動。 e. 按一下 標記為已解決。

事件被標記為已解決後，事件會移至已解決事件清單。

3. 選用：在 附註和更新 區域中，新增關於您如何處理該事件的附註，然後按一下 發布。

在 **Active IQ Unified Manager** 中將事件指派給特定使用者

您可以將未指派的事件指派給自己或其他使用者，包括遠端使用者。如有需要，您可以將已指派的事件重新指派給其他使用者。例如，當儲存設備物件頻繁發生問題時，您可以將這些問題的事件指派給管理該物件的使用者。

開始之前

- 使用者的姓名和電子郵件 ID 必須設定正確。
- 您必須擁有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下 事件管理。
2. 在「事件管理」清單頁面中，選取一或多個您要指派的事件。
3. 請選擇以下選項之一來指派事件：

如果您想將事件分配給.....	然後這樣做.....
您自己	點選 指派給 > 我。

如果您想將事件分配給.....	然後這樣做.....
另一位使用者	a. 點選 指派給 > 其他使用者。 b. 在「指派擁有者」對話方塊中，輸入使用者名稱，或從下拉式清單中選取使用者。 c. 按一下 指派。 系統會向使用者發送電子郵件通知。 如果您未輸入使用者名稱或從下拉清單中選取使用者，並按一下指派，則該事件將保持未指派狀態。

在 **Active IQ Unified Manager** 中停用不需要的事件

所有事件預設啟用。您可以全域停用事件，以防止產生環境中不重要事件的通知。如果您想要恢復接收某些事件的通知，可以重新啟用這些已停用的事件。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

停用事件後，系統中先前產生的事件將被標記為過時，並且不會觸發針對這些事件設定的警報。啟用已停用的事件後，這些事件的通知將從下一個監控週期開始產生。

當您停用物件的事件（例如 `vol offline`事件），然後稍後再啟用該事件時， Unified Manager 不會為事件處於停用狀態時離線的物件產生新事件。Unified Manager 僅在重新啟用事件後物件狀態發生變更時，才會產生新事件。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 事件設定。
2. 在 事件設定 頁面中，選擇下列選項之一以停用或啟用事件：

如果您想要.....	然後這樣做.....
停用事件	a. 按一下 **Disable** 。 b. 在「停用事件」對話方塊中，選擇事件嚴重性。 c. 在「比對事件」欄中，根據事件嚴重性選擇要停用的事件，然後按一下右箭頭將這些事件移至「停用事件」欄位。 d. 點選 儲存並關閉。 e. 確認您已停用的事件是否顯示在「事件設定」頁面的清單檢視中。
啟用事件	a. 選取您要啟用的一個或多個事件的核取方塊。 b. 按一下 **Enable** 。

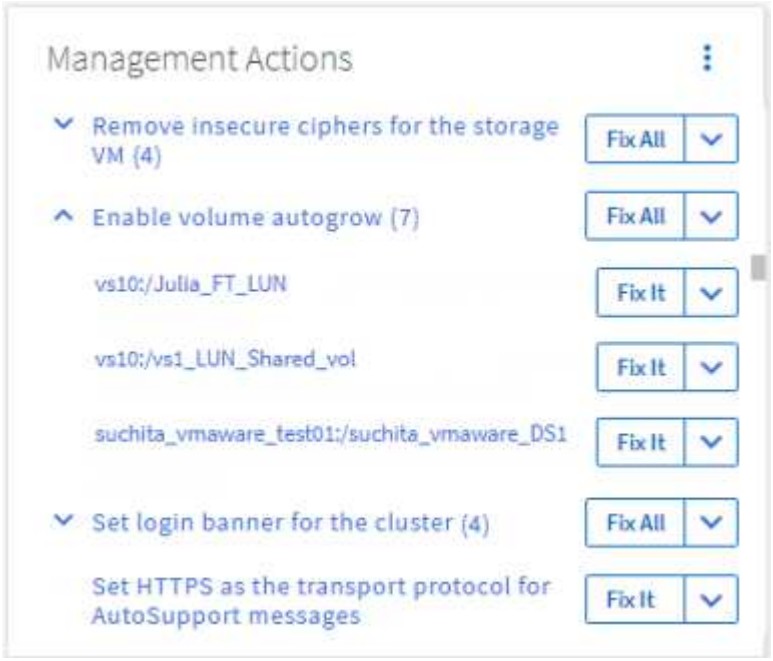
使用 **Active IQ Unified Manager** 中的自動修復功能來解決問題

Unified Manager 可以對某些事件進行全面診斷，並透過 **Fix It** 按鈕提供單一解決方案。如有解決方案，則會顯示在儀表板、事件詳情頁面以及左側導覽功能表的「工作負載分析」選項中。

大多數事件都有多種可能的解決方案，這些方案會顯示在事件詳情頁面中，以便您可以使用 ONTAP System Manager 或 ONTAP CLI 實作最佳解決方案。當 Unified Manager 確定只有單一解決方案可以解決問題，並且可以使用 ONTAP CLI 命令解決該問題時，則會提供 **Fix It** 行動。

步驟

1. 若要檢視可從*儀表板*修復的事件，請點選*儀表板*。



2. 若要解決 Unified Manager 可以修復的任何問題，請按一下 **Fix It** 按鈕。若要修復多個物件上存在的問題，請按一下 **Fix All** 按鈕。

有關可透過自動修復解決的問題資訊，請參閱"Unified Manager 可以解決哪些問題"。

在 **Active IQ Unified Manager** 中啟用並停用 **Active IQ** 事件報告

預設情況下， Active IQ 平台事件會在 Unified Manager 使用者介面中產生和顯示。如果您覺得這些事件過於「吵雜」，或者不想在 Unified Manager 中檢視這些事件，您可以停用這些事件的產生。如果您以後想恢復接收這些通知，可以隨時啟用它們。

開始之前

您必須擁有應用程式管理員角色。

停用此功能後，Unified Manager 將立即停止接收 Active IQ 平台事件。

當您啟用此功能時，Unified Manager 將根據叢集的時區，在午夜過後不久開始接收 Active IQ 平台事件。開始時間取決於 Unified Manager 何時收到來自各個叢集的 AutoSupport 訊息。

步驟

1. 在左側導覽窗格中，按一下 一般 > 功能設定。
2. 在「功能設定」頁面中，選擇以下選項之一，即可停用或啟用 Active IQ 平台事件：

如果您想要.....	然後這樣做.....
停用 Active IQ 平台事件	在 **Active IQ Portal Events** 面板中，將滑桿按鈕向左移動。
啟用 Active IQ 平台事件	在 **Active IQ Portal Events** 面板中，將滑桿按鈕向右移動。

在 **Active IQ Unified Manager** 中上傳新的 **Active IQ** 規則檔案

Unified Manager 會自動檢查新的 Active IQ 事件（規則）檔案，並在有較新規則時下載新檔案。但是，在沒有外部網路存取的站台中，您需要手動上傳規則檔案。

Active IQ 規則也稱為 Config Advisor （CA） 安全的規則。

當您在沒有網路連線的站台中安裝或升級 Unified Manager 到特定版本時，隨附的 Active IQ 規則會自動可供上傳。但是，建議您大約每個月從 NetApp 支援網站下載一次新的規則檔案，以確保產生更新的事件，並使您的儲存設備系統持續保持最佳效能。

開始之前

- 必須啟用 Active IQ 入口網站事件報告。此功能預設為啟用。如需詳細資訊，請參閱 "啟用 Active IQ 入口網站事件"。
- 您必須從 NetApp 支援網站下載規則檔案。

  規則檔案位於： https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

步驟

1. 在具有網路存取的電腦上，瀏覽至 NetApp 支援網站並下載目前的規則 `.zip`檔案。

   套裝組合的規則套件包含規則儲存庫、資料來源，以及一篇 NetApp 知識庫文章。

   在 Windows 系統上，在沒有網路連線的站台中，NetApp 知識庫文章預設不會與安裝程式套裝組合在一起。您可以從支援網站下載 *secure_rules.zip* 檔案，並將其上傳以檢視所有規則的知識庫文章。

2. 將規則檔案傳輸到您可以帶入安全的區域的媒體上，然後將其複製到安全的區域內的系統上。
3. 在左側導覽窗格中，按一下 儲存設備管理 > 事件設定。
4. 在 事件設定 頁面中，按一下 上傳規則 按鈕。
5. 在 上傳規則 對話方塊中，瀏覽並選取您下載的規則 `.zip`檔案，然後按一下 上傳。

   此程序可能需要幾分鐘。

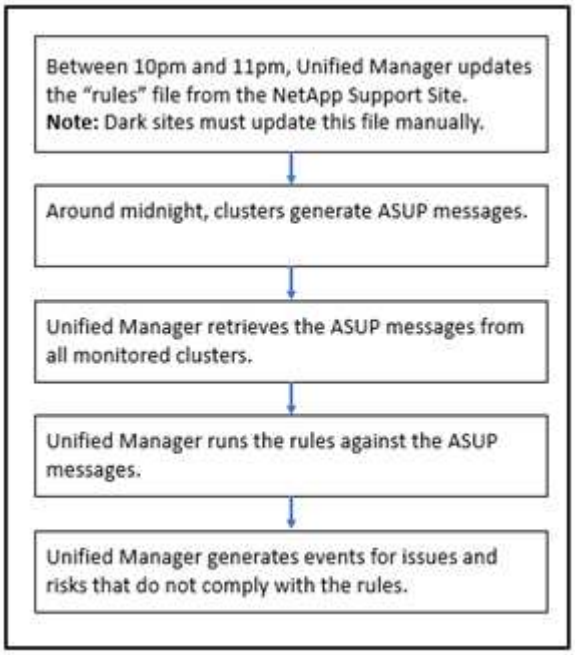
規則檔案會在 Unified Manager 伺服器上解壓縮。在您的受代管叢集於午夜過後產生 AutoSupport 檔案之後

，Unified Manager 會根據規則檔案檢查叢集，並視需要產生新的風險與發生事件。

如需詳細資訊，請參閱此知識庫（KB）文章： "如何在 Active IQ Unified Manager 中手動更新 AIQCASecure 規則"。

Active IQ Unified Manager 如何產生 Active IQ 平台事件

Active IQ 平台事件和風險會轉換為 Unified Manager 事件，如下圖所示。

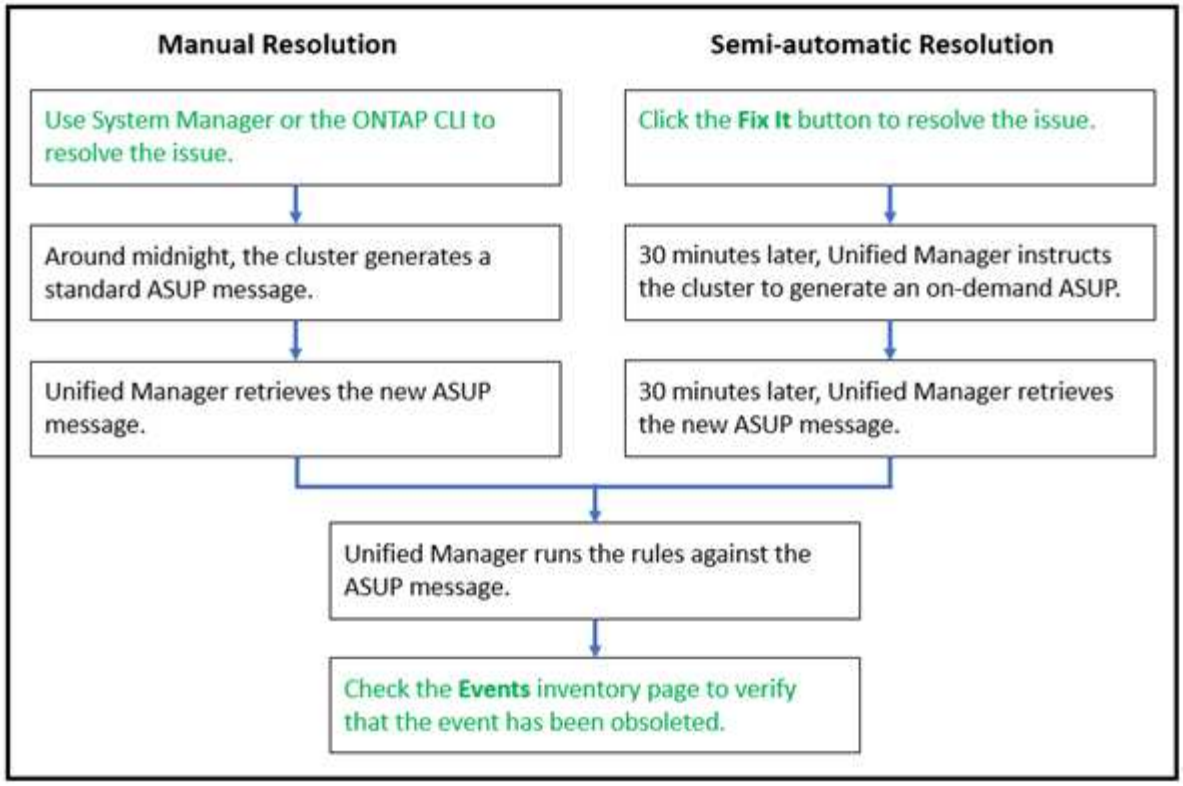


如您所見， Active IQ 平台上編譯的規則檔案保持最新狀態，叢集 AutoSupport 訊息每天都會產生， Unified Manager 每天都會更新事件清單。

在 Active IQ Unified Manager 中解決 Active IQ 平台事件

Active IQ 平台事件和風險與其他 Unified Manager 事件類似，因為它們可以指派給其他使用者進行解決，並且具有相同的可用狀態。但是，當您使用 **Fix It** 按鈕解決此類事件時，可以在數小時內驗證解決方案。

下圖顯示您在解決從 Active IQ 平台產生的事件時必須採取的行動（綠色）以及 Unified Manager 採取的行動（黑色）。



執行手冊解決時，您必須登入 System Manager 或 ONTAP 命令列介面來修正問題。只有在叢集於午夜產生新的 AutoSupport 訊息後，您才能驗證問題。

使用 **Fix It** 按鈕執行半自動修復時，您可以在幾個小時內驗證修復是否成功。

在 **Active IQ Unified Manager** 中設定事件保留設定

您可以指定事件在 Unified Manager 伺服器中保留的月數，超過該月數事件將會自動刪除。

開始之前

您必須擁有應用程式管理員角色。

保留事件超過 6 個月可能會影響伺服器效能，因此不建議這樣做。

步驟

1. 在左側導覽窗格中，按一下 一般 > 資料保留。
2. 在 資料保留 頁面中，選擇事件保留區域中的滑桿，將其移至事件應保留的月數，然後按一下 儲存。

什麼是 **Unified Manager** 維護所需時間

了解 **Active IQ Unified Manager** 的維護所需時間

您可以定義一個 Unified Manager 維護所需時間，以便在排定叢集維護時，在特定時間內抑制事件和警報，避免收到大量不必要的通知。

維護所需時間開始時，事件管理清單頁面會發布一則「物件維護所需時間已開始」事件。維護所需時間結束後，

此事件將自動失效。

在維護所需時間期間，與該叢集上所有物件相關的事件仍會產生，但它們不會顯示在任何使用者介面頁面中，也不會針對這些事件傳送任何警報或其他類型的通知。不過，您可以透過在「事件管理」清單頁面上選取其中一個「檢視」選項，來檢視在維護所需時間期間為所有儲存設備物件所產生的事件。

您可以排程在未來啟動維護所需時間，您可以變更已排程維護所需時間的開始和結束時間，也可以取消已排程的維護所需時間。

安排維護所需時間以停用 **Active IQ Unified Manager** 中的叢集事件通知

如果您有叢集的計畫性停機（例如，升級叢集或移動其中一個節點），則可以透過排程 Unified Manager 維護所需時間，來抑制通常在該時間範圍內產生的事件和警報。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

在維護所需時間期間，與該叢集上所有物件相關的事件仍會產生，但不會出現在事件頁面中，也不會針對這些事件傳送任何警報或其他類型的通知。

您為維護所需時間輸入的時間是以 Unified Manager 伺服器的時間為準。

步驟

1. 在左側導覽窗格中，按一下 儲存管理 > 叢集設定。
2. 在叢集的「維護模式」列中，選擇滑桿按鈕並將其向右移動。

   日曆視窗隨即顯示。

3. 選擇維護所需時間的開始和結束日期與時間，然後按一下 套用。

   滑桿按鈕旁邊會顯示「已排程」字樣。

當到達開始時間時，叢集將進入維護模式，並產生「物件維護所需時間已啟動」事件。

在 **Active IQ Unified Manager** 中變更或取消排定的維護所需時間

如果您已設定 Unified Manager 維護所需時間在未來進行，您可以變更開始時間和結束時間，或取消維護所需時間的進行。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

如果您在排定的維護所需時間結束時間之前完成了叢集維護，並且想要再次開始接收來自叢集的事件和警示，則取消目前正在執行的維護所需時間會很有用。

步驟

1. 在左側導覽窗格中，按一下 儲存管理 > 叢集設定。
2. 在叢集的 維護模式 欄位中：

如果您想要.....	執行此步驟.....
變更排定的維護所需時間的時間範圍	a. 點選滑桿按鈕旁的「已排程」字樣。 b. 變更開始和/或結束日期和時間，然後按一下 套用。
延長作用中維護所需時間	a. 點選滑桿按鈕旁的「作用中」字樣。 b. 變更結束日期和時間，然後按一下 套用。
取消排定的維護所需時間	選擇滑桿按鈕並將其向左移動。
取消作用中的維護所需時間	選擇滑桿按鈕並將其向左移動。

在 **Active IQ Unified Manager** 中查看維護所需時間期間產生的事件

如有需要，您可以檢視在 Unified Manager 維護所需時間期間為所有儲存設備物件產生的事件。維護所需時間結束且所有系統資源皆已恢復運作後，大多數事件將顯示為「已過時」狀態。

開始之前

在任何事件可用之前，至少必須完成一個維護所需時間。

預設情況下，維護所需時間期間發生的事件不會顯示在事件管理清單頁面上。

步驟

1. 在左側導覽窗格中，按一下 事件。

   預設情況下，所有作用中（新建和已確認）事件都會顯示在事件管理清單頁面上。

2. 從「檢視」窗格中，選取 維護期間產生的所有事件 選項。

   顯示過去 7 天內從所有維護所需時間工作階段與所有叢集觸發的事件清單。

3. 如果單一叢集有多個維護所需時間，您可以按一下 觸發時間 日曆圖示，然後選取您有興趣檢視的維護所需時間事件的期間。

在 **Active IQ Unified Manager** 中管理主機系統資源事件

Unified Manager 包含一項服務，用於監控安裝 Unified Manager 的主機系統上的資源問題。例如，主機系統可用磁碟空間不足或記憶體容量不足等問題可能會觸發管理站台事件，這些事件會以橫幅訊息的形式顯示在使用者介面頂部。

管理站事件表示安裝了 Unified Manager 的主機系統有問題。管理站問題的範例包括：主機系統磁碟空間不足；Unified Manager 錯失常規資料收集週期；以及由於已啟動下一次收集輪詢而導致統計資料分析未完成或延遲完成。

與所有其他 Unified Manager 事件訊息不同，這些特定的管理站警告和關鍵事件會顯示在橫幅訊息中。

步驟

1. 若要檢視管理站台事件資訊，請執行這些行動：

如果您想要.....	這樣做.....
檢視事件詳細資料	按一下事件橫幅以顯示事件詳細資料頁面，其中包含針對該問題的建議解決方案。
檢視所有管理站台事件	a. 在左側導覽窗格中，按一下 事件管理。 b. 在事件管理庫存頁面的篩選器窗格中，按一下來源類型清單中「Management Station」的方塊。

進一步了解事件

Active IQ Unified Manager 中的事件狀態

事件狀態有助於您確定是否需要採取適當的修正行動。事件狀態可以是「新建」、「已確認」、「已解決」或「已過時」。請注意，「新建」和「已確認」事件均被視為作用中事件。

事件狀態如下：

- 新增

  新事件的狀態。

- 已確認

  當您確認事件時的事件狀態。

- 已解決

  事件被標記為已解決時的狀態。

- 已過時

  事件自動修正或事件原因不再有效時的狀態。

  您無法確認或解決已過時的事件。

事件的不同狀態範例

以下範例說明手冊和自動事件狀態變更。

當「叢集無法連線」事件觸發時，事件狀態為「新增」。確認事件後，事件狀態會變更為「已確認」。採取適當的修正行動後，您必須將事件標記為已解決。然後事件狀態會變更為「已解決」。

如果 Cluster Not Reachable 事件是由於停電所產生，則在恢復供電後，叢集無需任何系統管理員介入即可開始運作。因此，Cluster Not Reachable 事件不再有效，且事件狀態會在下一個監控週期中變更為過時。

當事件處於「已過時」或「已解決」狀態時，Unified Manager 會傳送警報。警報的電子郵件主旨列和電子郵件內容會提供有關事件狀態的資訊。SNMP 陷阱也包含有關事件狀態的資訊。

了解 **Active IQ Unified Manager** 中的事件嚴重性類型

每個事件都與一個嚴重性類別相關聯，以幫助您確定需要立即修正行動的事件的優先順序。

- 關鍵

  發生問題，如果不立即採取修正行動，可能會導致服務中斷。

  效能關鍵事件僅由使用者定義的臨界值傳送。

- 錯誤

  事件來源仍在運作；但是，需要修正行動以避免服務中斷。

- 警告

  事件來源發生了您應該感知的事件，或者叢集物件的效能計數器超出正常範圍，應該加以監控以確保其不會達到關鍵嚴重性。此嚴重程度的事件不會導致服務中斷，可能不需要立即修正行動。

  效能警告事件是從使用者定義、系統定義或動態臨界值所傳送。

- 資訊

  當發現新物件或執行使用者行動時，就會觸發此事件。例如，當刪除任何儲存設備物件或進行任何組態變更時，都會產生嚴重性類別為「資訊」的事件。

  當 ONTAP 偵測到組態變更時，資訊事件會直接從 ONTAP 傳送。

了解 **Active IQ Unified Manager** 中的事件影響級別

每個事件都與一個影響層級（事故、風險、事件或升級）相關聯，以幫助您確定需要立即修正行動的事件的優先順序。

- 事件

  事故是指可能導致叢集停止向用戶端提供資料並耗盡資料儲存空間的一組事件。影響層級為「事故」的事件最為嚴重。應立即採取修正行動以避免服務中斷。

- 風險

  風險是指可能導致叢集停止向用戶端提供資料並耗盡資料儲存空間的一系列事件。影響層級為「風險」的事件可能導致服務中斷。可能需要採取修正行動。

- 事件

  事件是指儲存設備物件及其屬性的狀態或狀態變更。影響層級為「事件」的事件僅供參考，無需採取修正行動。

- 升級

  升級事件是 Active IQ 平台報告的特定類型的事件。這些事件顯示存在一些問題，需要升級 ONTAP 軟體、

節點韌體或作業系統軟體（針對安全性公告）才能解決。對於某些問題，您可能需要立即採取修正行動，而其他問題則可以等到下次排定的維護再處理。

了解 **Active IQ Unified Manager** 中的事件影響區域

事件分為六個影響領域（可用度、容量、組態、效能、保護和安全性），以便您可以專注於您負責的事件類型。

- 可用度

  可用度事件會在儲存設備物件離線、協定服務中斷、儲存設備故障轉移出現問題或硬體發生問題時通知您。

- 容量

  容量事件會在您的集合體、磁碟區、LUN 或命名空間接近或達到大小臨界值，或在您的環境中成長速度異常時通知您。

- 組態

  組態事件會通知您儲存設備物件的探索、刪除、新增、移除或重新命名。組態事件的影響層級為「事件」，嚴重性類別為「資訊」。

- 效能

  效能事件會通知您叢集上的資源、組態或活動狀況，這些狀況可能會對受監控儲存設備物件的資料儲存設備輸入或擷取速度產生不利影響。

- 保護

  保護事件會通知您涉及 SnapMirror 關係、目的地容量問題、SnapVault 關係問題或保護作業問題的事件或風險。任何做為次要磁碟區與保護關係主機的 ONTAP 物件（尤其是 Aggregate、磁碟區和 SVM）都會歸類在保護影響區域中。

- 安全性

  安全性事件會根據在 "NetApp ONTAP 9 安全性強化指南"中定義的參數，通知您 ONTAP 叢集、儲存設備虛擬機器（SVM）和磁碟區的安全程度。

  此外，此區域還包含從 Active IQ 平台報告的升級事件。

Active IQ Unified Manager 如何計算物件狀態

物件狀態由目前處於「新建」或「已確認」狀態的最嚴重事件決定。例如，如果物件狀態為「錯誤」，則該物件的某個事件的嚴重性類別為「錯誤」。當採取修正行動後，事件狀態將變為「已解決」。

了解 **Active IQ Unified Manager** 中的動態效能事件

對於動態效能事件，「事件詳細資料」頁面的「系統診斷」區段會列出延遲最高，或對發生爭用之叢集元件使用率最高的前幾大工作負載。

效能統計資料是根據從偵測到效能事件到最後一次分析該事件的時間。圖表也會顯示發生爭用之叢集元件的歷史效能統計資料。

例如，您可以識別元件使用率高的工作負載，從而確定將哪些工作負載遷移到使用率較低的元件。遷移工作負載會減少目前元件的工作量，並可能使該元件脫離爭用狀態。本節頂部顯示的是偵測到事件及上次分析的時間和日期範圍。對於作用中事件（新事件或已確認事件），上次分析時間會更新。

將游標停留在延遲和活動圖表上時，圖表會顯示排名最高的工作負載名稱。按一下圖表右側的「工作負載類型」選單，您可以根據工作負載在事件中的角色對其進行排序（包括 *sharks*、*bullies* 或 *victims*），並顯示有關其延遲及其在競爭叢集元件上使用情況的詳細資訊。您可以將實際值與預期值進行比較，以查看工作負載何時超出其預期的延遲或使用範圍。如需詳細資訊，請參閱 "Unified Manager 監控的工作負載類型"。

當您依延遲的峰值偏差進行排序時，系統定義的工作負載不會顯示在表格中，因為延遲僅適用於使用者定義的工作負載。延遲值極低的工作負載不會顯示在表格中。

如需有關動態效能臨界值的詳細資訊，請參閱"分析動態效能閾值事件"。

如需有關 Unified Manager 如何對工作負載進行排名並決定排序順序的資訊，請參閱 "Unified Manager 如何決定事件的效能影響"。

圖表中的資料顯示上次分析事件前 24 小時的效能統計資料。每個工作負載的實際值和預期值是根據工作負載參與事件的時間而定。例如，工作負載可能在偵測到事件之後才參與事件，因此其效能統計資料可能與偵測到事件時的值不符。依預設，工作負載會依延遲的峰值（最高）偏差排序。

由於 Unified Manager 最多保留 30 天的 5 分鐘歷史效能和事件資料，如果事件超過 30 天，則不會顯示任何效能資料。

- 工作負載排序欄
  - 延遲圖表

    顯示該事件對上次分析期間工作負載延遲的影響。

  - 元件使用狀況欄

    顯示有關爭用叢集元件的工作負載使用情況詳細資訊。在圖表中，實際使用情況以藍線表示。紅色長條會突顯事件持續時間，從偵測時間到上次分析時間。如需詳細資訊，請參閱 "工作負載效能測量值"。

    對於網路元件，由於網路效能統計資料來自叢集外的活動，因此不顯示此欄。

  - 組件使用情況

    顯示網路處理、資料處理和彙總元件的使用率歷史記錄（以百分比表示），或顯示 QoS 原則群組元件的活動歷史記錄（以百分比表示）。網路或互連元件不會顯示圖表。您可以指向統計資料，以檢視特定時間點的使用情況統計資料。

  - 總寫入 **MB/s** 歷史記錄

    僅針對 MetroCluster 資源元件，顯示在 MetroCluster 組態中鏡射至合作夥伴叢集的所有 Volume 工作負載的總寫入處理量，單位為每秒百萬位元組 (MBps)。

  - 事件歷程

顯示紅色陰影線條，指示衝突元件的歷史事件。對於已過時的事件，圖表會顯示在偵測到所選事件之前和解決之後發生的事件。

Active IQ Unified Manager 偵測到設定變更

Unified Manager 會監控叢集的組態變更，以協助您判斷變更是否可能導致或促成效能事件。Performance Explorer 頁面會顯示變更事件圖示（●），以指出偵測到變更的日期和時間。

您可以在 Performance Explorer 頁面和 Workload Analysis 頁面中審查效能圖表，以查看變更事件是否影響了所選叢集物件的效能。如果偵測到變更的時間與效能事件同時或相近，則該變更可能導致了問題，進而觸發事件警報。

Unified Manager 可以偵測到下列變更事件，這些事件被歸類為資訊事件：

- Volume 在 Aggregate 之間移動。

  Unified Manager 可以偵測搬移何時正在進行、已完成或失敗。如果在 Volume 搬移期間 Unified Manager 停機，當它恢復運作時，會偵測到 Volume 搬移並顯示其變更事件。

- 包含一個或多個受監控工作負載的 QoS 原則群組的處理量（MB/s 或 IOPS）限制會變更。

  更改原則群組限制可能會導致延遲（回應時間）出現間歇性峰值，這也可能觸發原則群組的事件。延遲會逐漸恢復正常，由峰值引起的任何事件都會失效。

- HA 配對中的一個節點接管或歸還其合作夥伴節點的儲存設備。

  Unified Manager 可以偵測到接管、部分接管或歸還作業何時完成。如果接管是由發生當機的節點所引起，Unified Manager 不會偵測到該事件。

- ONTAP 升級或回復作業已成功完成。

  顯示舊版本和新版本。

事件和嚴重性類型列表

了解 **Active IQ Unified Manager** 中的彙總事件

Aggregate 事件提供有關 Aggregate 狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
集合體離線（ocumEvtAggregateStateOffline）	事件	彙總	關鍵

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
集合體失敗（ocumEvtAggregateStateFailed）	事件	彙總	關鍵
集合體受限（ocumEvtAggregateStateRestricted）	風險	彙總	警告
Aggregate 重構（ocumEvtAggregateRaidStateReconstructing）	風險	彙總	警告
集合體降級（ocumEvtAggregateRaidStateDegraded）	風險	彙總	警告
雲端層部分可達（ocumEventCloudTierPartiallyReachable）	風險	彙總	警告
雲端層無法連線（ocumEventCloudTierUnreachable）	風險	彙總	錯誤
雲端層存取遭拒，無法進行 Aggregate 重新配置 *（arlNetraCaCheckFailed）	風險	彙總	錯誤
在儲存容錯移轉期間 Aggregate 重新定位的雲端層存取遭拒 *(gbNetraCaCheckFailed)	風險	彙總	錯誤
MetroCluster 遺留的集合體（ocumEvtMetroClusterAggregateLeftBehind）	風險	彙總	錯誤
MetroCluster 集合體鏡射降級（ocumEvtMetroClusterAggregateMirrorDegraded）	風險	彙總	錯誤

影響區域：容量

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
集合體空間幾乎已滿（ocumEvtAggregateNearlyFull）	風險	彙總	警告
集合體空間已滿（ocumEvtAggregateFull）	風險	彙總	錯誤

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
Aggregate 滿載前天數（ocumEvtAggregateDaysUntilFullSoon）	風險	彙總	錯誤
集合體過度配置（ocumEvtAggregateOvercommitted）	風險	彙總	錯誤
集合體幾乎過度配置（ocumEvtAggregateAlmostOvercommitted）	風險	彙總	警告
Aggregate Snapshot 快照技術保留空間已滿（ocumEvtAggregateSnapReserveFull）	風險	彙總	警告
Aggregate 成長率異常（ocumEvtAggregateGrowthRateAbnormal）	風險	彙總	警告

影響區域：組態

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
已發現 Aggregate（不適用）	事件	彙總	資訊
集合體已重新命名（不適用）	事件	彙總	資訊
Aggregate 已刪除（不適用）	事件	節點	資訊

影響領域：效能

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
Aggregate IOPS 臨界閾值已突破（ocumAggregateIopsIncident）	事件	彙總	關鍵
Aggregate IOPS 警告臨界值已遭違反（ocumAggregateIopsWarning）	風險	彙總	警告
Aggregate MB/s 嚴重臨界值已違反（ocumAggregateMbpsIncident）	事件	彙總	關鍵

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
Aggregate MB/s 警告臨界值已違反（ocumAggregateMbpsWarning）	風險	彙總	警告
集合體延遲臨界閾值已突破（ocumAggregateLatencyIncident）	事件	彙總	關鍵
集合體延遲警告臨界值已遭違反（ocumAggregateLatencyWarning）	風險	彙總	警告
已使用的 Aggregate 效能容量已突破臨界閾值（ocumAggregatePerfCapacityUsedIncident）	事件	彙總	關鍵
Aggregate 已使用的效能容量警告臨界值已突破（ocumAggregatePerfCapacityUsedWarning）	風險	彙總	警告
集合體使用率臨界閾值已突破（ocumAggregateUtilizationIncident）	事件	彙總	關鍵
集合體使用率警告臨界值已違反（ocumAggregateUtilizationWarning）	風險	彙總	警告
Aggregate 磁碟過度使用臨界值已突破（ocumAggregateDisksOverUtilizedWarning）	風險	彙總	警告
集合體動態臨界值突破（ocumAggregateDynamicEventWarning）	風險	彙總	警告

了解 **Active IQ Unified Manager** 中的叢集事件

叢集事件提供有關叢集狀態的資訊，使您能夠監控叢集是否有潛力問題。這些事件依影響區域分組，並包含事件名稱、設陷名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
叢集缺少備用磁碟（ocumEvtDisksNoSpares）	風險	叢集	警告
叢集無法連線（ocumEvtClusterUnreachable）	風險	叢集	錯誤
叢集監控失敗（ocumEvtClusterMonitoringFailed）	風險	叢集	警告
叢集 FabricPool 授權容量限制已超出（ocumEvtExternalCapacityTierSpaceFull）	風險	叢集	警告
NVMe-oF 寬限期已開始 *（nvmfGracePeriodStart）	風險	叢集	警告
NVMe-oF 寬限期已啟動 *（nvmfGracePeriodActive）	風險	叢集	警告
NVMe-oF 寬限期已過期 *(nvmfGracePeriodExpired)	風險	叢集	警告
物件維護時段已啟動（objectMaintenanceWindowStarted）	事件	叢集	關鍵
物件維護時段已結束（objectMaintenanceWindowEnded）	事件	叢集	資訊
MetroCluster 剩餘的備用磁碟（ocumEvtSpareDiskLeftBehind）	風險	叢集	錯誤
MetroCluster 自動非計劃切換已停用（ocumEvtMccAutomaticUnplannedSwitchOverDisabled）	風險	叢集	警告
叢集使用者密碼已更改 *(cluster.passwd.changed)	事件	叢集	資訊

影響區域：容量

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
叢集容量不平衡臨界值已違反（ocumConformanceNodeImbalanceWarning）	風險	叢集	警告
叢集雲端層規劃（clusterCloudTierPlanningWarning）	風險	叢集	警告
FabricPool 鏡像複寫重新同步完成*(waflCaResyncComplete)	事件	叢集	警告
FabricPool 空間幾乎已滿*（fabricpoolNearlyFull）	風險	叢集	錯誤

影響區域：組態

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
節點已新增（不適用）	事件	叢集	資訊
節點已移除（不適用）	事件	叢集	資訊
叢集已移除（不適用）	事件	叢集	資訊
叢集新增失敗（不適用）	事件	叢集	錯誤
叢集名稱已變更（不適用）	事件	叢集	資訊
收到緊急 EMS（不適用）	事件	叢集	關鍵
收到關鍵 EMS（不適用）	事件	叢集	關鍵
已收到 EMS 警報（不適用）	事件	叢集	錯誤
收到 EMS 錯誤（不適用）	事件	叢集	警告
收到 EMS 警告（不適用）	事件	叢集	警告
偵錯 EMS 已接收（不適用）	事件	叢集	警告
已收到 EMS 通知（不適用）	事件	叢集	警告
收到資訊性 EMS（不適用）	事件	叢集	警告

ONTAP EMS 事件分為三個 Unified Manager 事件嚴重性層級。

Unified Manager 事件嚴重層級	ONTAP EMS 事件嚴重層級

關鍵	緊急狀況 關鍵
錯誤	警示
警告	錯誤 警告 偵錯 注意 資訊

影響領域：效能

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
叢集負載不平衡臨界值已突破（）	風險	叢集	警告
叢集 IOPS 危急臨界值已突破（ocumClusterIopsIncident）	事件	叢集	關鍵
叢集 IOPS 警告臨界值已違反（ocumClusterIopsWarning）	風險	叢集	警告
叢集 MB/s 嚴重臨界值已違反（ocumClusterMbpsIncident）	事件	叢集	關鍵
叢集 MB/s 警告臨界值已突破（ocumClusterMbpsWarning）	風險	叢集	警告
叢集動態臨界值已違反（ocumClusterDynamicEventWarning）	風險	叢集	警告

影響領域：安全性

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
AutoSupport HTTPS 傳輸已停用（ocumClusterASUPHttpsConfiguredDisabled）	風險	叢集	警告

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
日誌轉送未加密（ocumClusterAuditLogUnencrypted）	風險	叢集	警告
預設本機管理員使用者已啟用（ocumClusterDefaultAdminEnabled）	風險	叢集	警告
FIPS 模式已停用（ocumClusterFipsDisabled）	風險	叢集	警告
登入橫幅已停用（ocumClusterLoginBannerDisabled）	風險	叢集	警告
登入橫幅已更改（ocumClusterLoginBannerChanged）	風險	叢集	警告
日誌轉送目的地已變更（ocumLogForwardDestinationsChanged）	風險	叢集	警告
NTP 伺服器名稱已變更（ocumNtpServerNamesChanged）	風險	叢集	警告
NTP 伺服器數量低（securityConfigNTPServerCountLowRisk）	風險	叢集	警告
叢集對等通訊未加密（ocumClusterPeerEncryptionDisabled）	風險	叢集	警告
SSH 正在使用不安全的加密演算法（ocumClusterSSHInsecure）	風險	叢集	警告
Telnet 協定已啟用（ocumClusterTelnetEnabled）	風險	叢集	警告
部分 ONTAP 使用者帳號的密碼使用較不安全的 MD5 雜湊函數（ocumClusterMD5PasswordHashUsed）	風險	叢集	警告
叢集使用自簽名憑證（ocumClusterSelfSignedCertificate）	風險	叢集	警告

事件名稱（設陷名稱）	影響層級	來源類型	嚴重程度
叢集遠端 Shell 已啟用（ocumClusterRshDisabled）	風險	叢集	警告
叢集憑證即將過期（ocumEvtClusterCertificateAboutToExpire）	風險	叢集	警告
叢集憑證已過期（ocumEvtClusterCertificateExpired）	風險	叢集	錯誤

了解 **Active IQ Unified Manager** 中的磁碟事件

磁碟事件提供有關磁碟狀態的資訊，以便您監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Flash 磁碟 - 備用區塊幾乎已用完（ocumEvtClusterFlashDiskFewerSpareBlockError）	風險	叢集	錯誤
Flash 磁碟 - 無備用區塊（ocumEvtClusterFlashDiskNoSpareBlockCritical）	事件	叢集	關鍵
部分未指派的磁碟（ocumEvtClusterUnassignedDisksSome）	風險	叢集	警告
部分磁碟故障（ocumEvtDisksSomeFailed）	事件	叢集	關鍵

了解 **Active IQ Unified Manager** 中的機櫃事件

機櫃事件提供資料中心內磁碟櫃機櫃的狀態訊息，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
磁碟櫃風扇故障（ocumEvtShelfFanFailed）	事件	儲存機櫃	關鍵

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
磁碟櫃電源故障（ocumEvtShelfPowerSupplyFailed）	事件	儲存機櫃	關鍵
磁碟櫃多路徑未設定（ocumDiskShelfConnectivityNotInMultiPath） 此事件不適用於： • 處於 MetroCluster 組態的叢集 • 以下平台：FAS2554、FAS2552、FAS2520 和 FAS2240	風險	節點	警告
磁碟櫃路徑故障（ocumDiskShelfConnectivityPathFailure）	風險	儲存機櫃	警告

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
已發現磁碟櫃（不適用）	事件	節點	資訊
磁碟櫃已移除（不適用）	事件	節點	資訊

了解 **Active IQ Unified Manager** 中的風扇事件

風扇事件提供資料中心節點上風扇的狀態資訊，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
一個或多個故障風扇（ocumEvtFansOneOrMoreFailed）	事件	節點	關鍵

了解 **Active IQ Unified Manager** 中的快閃記憶卡事件

Flash 卡事件提供有關資料中心節點上已安裝 Flash 卡的狀態資訊，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Flash 卡離線（ocumEvtFlashCardOffline）	事件	節點	關鍵

了解 **Active IQ Unified Manager** 中的 **inode** 事件

inode 事件會在 inode 已滿或接近已滿時提供資訊，以便您監控潛力問題。事件按影響區域分組，包含事件和設陷名稱、影響層級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Inodes 幾乎已滿（ocumEvtInodesAlmostFull）	風險	磁碟區	警告
Inodes Full（ocumEvtInodesFull）	風險	磁碟區	錯誤

Active IQ Unified Manager 中的網路介面事件

網路介面事件提供有關網路介面（LIF）狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
網路介面狀態已關閉（ocumEvtLifStatusDown）	風險	介面	錯誤
FC/FCoE 網路介面狀態關閉（ocumEvtFCLifStatusDown）	風險	介面	錯誤
網路介面無法容錯移轉（ocumEvtLifFailoverNotPossible）	風險	介面	警告
網路介面不在主連接埠（ocumEvtLifNotAtHomePort）	風險	介面	警告

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
網路介面路由未設定（不適用）	事件	介面	資訊

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
網路介面 MB/s 臨界閾值已突破（ocumNetworkLifMbpsIncident）	事件	介面	關鍵
網路介面 MB/s 警告閾值已違反（ocumNetworkLifMbpsWarning）	風險	介面	警告
FC 網路介面 MB/s 臨界閾值已突破（ocumFcpLifMbpsIncident）	事件	介面	關鍵
FC 網路介面 MB/s 警告閾值已突破（ocumFcpLifMbpsWarning）	風險	介面	警告
NVMf FC 網路介面 MB/s 臨界閾值已突破（ocumNvmfFcLifMbpsIncident）	事件	介面	關鍵
NVMf FC 網路介面 MB/s 警告閾值已突破（ocumNvmfFcLifMbpsWarning）	風險	介面	警告

了解 **Active IQ Unified Manager** 中的 **LUN** 事件

LUN 事件提供有關 LUN 狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
LUN 離線（ocumEvtLunOffline）	事件	LUN	關鍵
LUN 已銷毀 *（lunDestroy）	事件	LUN	資訊
在 igroup（igroupUnsupportedOsType）中對應不支援之作業系統的 LUN	事件	LUN	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
存取 LUN 的單一主動路徑（ocumEvtLunSingleActivePath）	風險	LUN	警告
沒有可存取 LUN 的作用中路徑（ocumEvtLunNotReachable）	事件	LUN	關鍵
沒有存取 LUN 的最佳化路徑（ocumEvtLunOptimizedPathInactive）	風險	LUN	警告
沒有從 HA 合作夥伴存取 LUN 的路徑（ocumEvtLunHaPathInactive）	風險	LUN	警告
HA 對中的一個節點沒有存取 LUN 的路徑（ocumEvtLunNodePathStatusDown）	風險	LUN	錯誤

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
LUN Snapshot 快照技術副本空間不足（ocumEvtLunSnapshotNotPossible）	風險	磁碟區	警告

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
在 igroup（igroupUnsupportedOsType）中對應不支援之作業系統的 LUN	風險	LUN	警告

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
LUN IOPS 臨界閾值已突破（ocumLunIopsIncident）	事件	LUN	關鍵
LUN IOPS 警告閾值已突破（ocumLunIopsWarning）	風險	LUN	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
LUN MB/s 嚴重臨界值已遭違反（ocumLunMbpsIncident）	事件	LUN	關鍵
LUN MB/s 警告閾值已突破（ocumLunMbpsWarning）	風險	LUN	警告
LUN 延遲 ms/op 嚴重臨界值已突破（ocumLunLatencyIncident）	事件	LUN	關鍵
LUN 延遲 ms/op 警告臨界值已違反（ocumLunLatencyWarning）	風險	LUN	警告
LUN 延遲和 IOPS 臨界閾值已違反（ocumLunLatencyIopsIncident）	事件	LUN	關鍵
LUN 延遲和 IOPS 警告臨界值已違反（ocumLunLatencyIopsWarning）	風險	LUN	警告
LUN 延遲和 MB/s 臨界閾值已突破（ocumLunLatencyMbpsIncident）	事件	LUN	關鍵
LUN 延遲和 MB/s 警告閾值已突破（ocumLunLatencyMbpsWarning）	風險	LUN	警告
LUN 延遲和 Aggregate 效能容量使用情況已超過臨界閾值（ocumLunLatencyAggregatePerfCapacityUsedIncident）	事件	LUN	關鍵
LUN 延遲和 Aggregate 效能容量使用情況警告閾值已突破（ocumLunLatencyAggregatePerfCapacityUsedWarning）	風險	LUN	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
LUN 延遲和 Aggregate 使用率已超過嚴重臨界值（ocumLunLatencyAggregateUtilizationIncident）	事件	LUN	關鍵
LUN 延遲與 Aggregate 使用率警告臨界值已違反（ocumLunLatencyAggregateUtilizationWarning）	風險	LUN	警告
LUN 延遲和節點效能容量使用率已超過臨界閾值（ocumLunLatencyNodePerfCapacityUsedIncident）	事件	LUN	關鍵
LUN 延遲和節點效能容量使用量警告閾值已突破（ocumLunLatencyNodePerfCapacityUsedWarning）	風險	LUN	警告
LUN 延遲和節點效能容量已用 - 接管臨界閾值已突破（ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident）	事件	LUN	關鍵
LUN 延遲和節點效能容量已使用 - 接管警告閾值已突破（ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning）	風險	LUN	警告
LUN 延遲和節點利用率已突破臨界閾值（ocumLunLatencyNodeUtilizationIncident）	事件	LUN	關鍵
LUN 延遲與節點使用率警告臨界值已違反（ocumLunLatencyNodeUtilizationWarning）	風險	LUN	警告
QoS LUN 最大 IOPS 警告臨界值已違反（ocumQosLunMaxIopsWarning）	風險	LUN	警告
QoS LUN 最大 MB/s 警告臨界值已違反（ocumQosLunMaxMbpsWarning）	風險	LUN	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
工作負載 LUN 延遲臨界值已超出效能服務層級原則（ocumConformanceLatencyWarning）所定義的範圍	風險	LUN	警告

了解 **Active IQ Unified Manager** 中的管理站台事件

管理站事件提供有關安裝 Unified Manager 的伺服器狀態的資訊，以便您監控潛力問題。事件依影響區域分組，包括事件與陷阱名稱、影響層級、來源類型及嚴重性。

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
管理伺服器磁碟空間即將用完（ocumEvtUnifiedManagerDiskSpaceNearlyFull）	風險	管理站	警告
管理伺服器磁碟空間已滿（ocumEvtUnifiedManagerDiskSpaceFull）	事件	管理站	關鍵
管理伺服器記憶體不足（ocumEvtUnifiedManagerMemoryLow）	風險	管理站	警告
管理伺服器記憶體即將耗盡（ocumEvtUnifiedManagerMemoryAlmostOut）	事件	管理站	關鍵
MySQL 日誌檔案大小增加；需要重新啟動（ocumEvtMysqlLogFileSizeWarning）	事件	管理站	警告
總稽核日誌大小配置即將額滿	風險	管理站	警告
Syslog 伺服器憑證即將過期	風險	管理站	警告
Syslog 伺服器憑證已過期	風險	管理站	錯誤
稽核日誌檔案遭竄改	風險	管理站	警告
稽核日誌檔已刪除	風險	管理站	警告
Syslog 伺服器連線錯誤	風險	管理站	錯誤
Syslog 伺服器組態已更改	事件	管理站	警告

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
效能資料分析受到影響（ocumEvtUnifiedManagerDataMissingAnalyze）	風險	管理站	警告
效能資料收集受到影響（ocumEvtUnifiedManagerDataMissingCollection）	事件	管理站	關鍵

最後這兩個效能事件僅適用於 Unified Manager 7.2。如果其中任何一個事件處於「新增」狀態，然後您升級到較新版本的 Unified Manager 軟體，則這些事件不會自動清除。您需要手動將這些事件移至「已解決」狀態。

了解 **Active IQ Unified Manager** 中的 **MetroCluster Bridge** 事件

MetroCluster 橋接事件提供有關橋接器狀態的資訊，以便您可以在 FC 上的 MetroCluster 組態中監控潛力的問題。事件按影響區域分組，包括事件和 trap 名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
橋接器無法連線（ocumEvtBridgeUnreachable）	事件	MetroCluster 橋接器	關鍵
橋接溫度異常（ocumEvtBridgeTemperatureAbnormal）	事件	MetroCluster 橋接器	關鍵

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 連線事件

連線事件提供有關叢集元件之間，以及在透過 FC 的 MetroCluster 與透過 IP 的 MetroCluster 組態中叢集之間連線的資訊，以便您可以監控潛力問題。事件依影響區域分組，包括事件與 trap 名稱、影響層級、來源類型及嚴重性。

兩種組態中常見的事件

這些連線事件在透過 FC 的 MetroCluster 和透過 IP 的 MetroCluster 組態中都很常見。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
所有 MetroCluster 合作夥伴之間的連結皆已中斷（ocumEvtMetroClusterAllLinksBetweenPartnersDown）	事件	MetroCluster 關係	關鍵
MetroCluster 合作夥伴無法透過對等網路連線（ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork）	事件	MetroCluster 關係	關鍵
MetroCluster 災難復原能力受到影響（ocumEvtMetroClusterDRStatusImpacted）	風險	MetroCluster 關係	關鍵
MetroCluster 組態已切換（ocumEvtMetroClusterDRStatusImpacted）	風險	MetroCluster 關係	警告

MetroCluster FC 組態

這些事件與 FC 上的 MetroCluster 組態有關。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
所有交換器間連結中斷（ocumEvtMetroClusterAllISLBetweenSwitchesDown）	事件	MetroCluster 交換器間連接	關鍵
FC-SAS 橋接器至儲存設備堆疊連結中斷（ocumEvtBridgeSasPortDown）	事件	MetroCluster 橋接堆疊連線	關鍵
MetroCluster 組態部分切換（ocumEvtMetroClusterDRStatusPartiallyImpacted）	風險	MetroCluster 關係	錯誤
節點到 FC 交換器所有 FC-VI 互連連結中斷（ocumEvtMccNodeSwitchFcviLinksDown）	事件	MetroCluster 節點交換器連接	關鍵

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
節點至 FC 交換器的一個或多個 FC 啟動器連結中斷（ocumEvtMccNodeSwitchFcLinksOneOrMoreDown）	風險	MetroCluster 節點交換器連接	警告
節點至 FC 交換器的所有 FC 啟動器連結中斷（ocumEvtMccNodeSwitchFcLinksDown）	事件	MetroCluster 節點交換器連接	關鍵
交換器至 FC-SAS 橋接器 FC 連結中斷（ocumEvtMccSwitchBridgeFcLinksDown）	事件	MetroCluster 交換器橋接連線	關鍵
節點間所有 FC VI InterConnect 連結中斷（ocumEvtMccInterNodeLinksDown）	事件	節點間連線	關鍵
節點間一個或多個 FC VI InterConnect 連結斷線（ocumEvtMccInterNodeLinksOneOrMoreDown）	風險	節點間連線	警告
節點到橋接連結斷開（ocumEvtMccNodeBridgeLinksDown）	事件	節點橋接連線	關鍵
節點到儲存堆疊的所有 SAS 連結均已斷開（ocumEvtMccNodeStackLinksDown）	事件	節點堆疊連接	關鍵
節點到儲存堆疊的一個或多個 SAS 連結斷開（ocumEvtMccNodeStackLinksOneOrMoreDown）	風險	節點堆疊連接	警告

MetroCluster 透過 IP 組態

這些事件與 MetroCluster over IP 組態有關。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
MetroCluster IP 站點間連線狀態中斷（mccIntersiteconnectivityStatusDown）	風險	MetroCluster 關係	關鍵

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
MetroCluster-IP 節點至交換器連線離線（mccIpPortStatusOffline）	風險	節點	錯誤

了解 **Active IQ Unified Manager** 中的 **MetroCluster** 交換器事件

MetroCluster 交換器事件（針對 FC 上的 MetroCluster 組態）可提供有關 MetroCluster 交換器狀態的資訊，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
交換器溫度異常（ocumEvtSwitchTemperatureAbnormal）	事件	MetroCluster 交換器	關鍵
交換器無法連線（ocumEvtSwitchUnreachable）	事件	MetroCluster 交換器	關鍵
交換器風扇故障（ocumEvtSwitchFansOneOrMoreFailed）	事件	MetroCluster 交換器	關鍵
交換器電源故障（ocumEvtSwitchPowerSuppliesOneOrMoreFailed）	事件	MetroCluster 交換器	關鍵
交換器溫度感知器故障（ocumEvtSwitchTemperatureSensorFailed） 此事件僅適用於 Cisco 交換器。	事件	MetroCluster 交換器	關鍵

了解 **Active IQ Unified Manager** 中的 **NVMe** 命名空間事件

NVMe 命名空間事件提供有關命名空間狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重性。

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
NVMeNS 離線 *(nvmeNamespaceStatusOffline)	事件	命名空間	資訊
NVMeNS 線上 *(nvmeNamespaceStatusOnline)	事件	命名空間	資訊
NVMeNS 空間不足 *（nvmeNamespaceSpaceOutOfSpace）	風險	命名空間	警告
NVMeNS 銷毀 *(nvmeNamespaceDestroy)	事件	命名空間	資訊

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
NVMe 命名空間 IOPS 嚴重臨界值已突破（ocumNvmeNamespaceIopsIncident）	事件	命名空間	關鍵
NVMe 命名空間 IOPS 警告臨界值已違反（ocumNvmeNamespaceIopsWarning）	風險	命名空間	警告
NVMe 命名空間 MB/s 臨界閾值已突破（ocumNvmeNamespaceMbpsIncident）	事件	命名空間	關鍵
NVMe 命名空間 MB/s 警告閾值已突破（ocumNvmeNamespaceMbpsWarning）	風險	命名空間	警告
NVMe 命名空間延遲 ms/op 臨界閾值已突破（ocumNvmeNamespaceLatencyIncident）	事件	命名空間	關鍵
NVMe 命名空間延遲 ms/op 警告閾值已突破（ocumNvmeNamespaceLatencyWarning）	風險	命名空間	警告
NVMe 命名空間延遲和 IOPS 臨界閾值已突破（ocumNvmeNamespaceLatencyIopsIncident）	事件	命名空間	關鍵

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
NVMe 命名空間延遲和 IOPS 警告閾值已突破（ocumNvmeNamespaceLatencyIopsWarning）	風險	命名空間	警告
NVMe 命名空間延遲和 MB/s 臨界閾值已突破（ocumNvmeNamespaceLatencyMbpsIncident）	事件	命名空間	關鍵
NVMe 命名空間延遲和 MB/s 警告閾值已突破（ocumNvmeNamespaceLatencyMbpsWarning）	風險	命名空間	警告

了解 **Active IQ Unified Manager** 中的節點事件

節點事件提供有關節點狀態的資訊，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
節點根磁碟區空間幾乎已滿（ocumEvtClusterNodeRootVolumeSpaceNearlyFull）	風險	節點	警告
雲端 AWS MetaDataConnFail *（ocumCloudAwsMetadataConnFail）	風險	節點	錯誤
雲端 AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	風險	節點	錯誤
雲端 AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	風險	節點	錯誤
雲端 AWS IAMCredsNotFound *（ocumCloudAwsIamCredsNotFound）	風險	節點	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
雲端 AWS IAMCredsNotInitialized *（ocumCloudAwsIamCredsNotInitialized）	事件	節點	資訊
雲端 AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	風險	節點	錯誤
雲端 AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	風險	節點	錯誤
雲端分層主機無法解析 *(ocumObjstoreHostUnresolvable)	風險	節點	錯誤
雲端層叢集間網路介面中斷 *(ocumObjstoreInterClusterLifDown)	風險	節點	錯誤
其中一個 NFSv4 集區已耗盡 *(nbladeNfsv4PoolEXhaust)	事件	節點	關鍵
要求不符雲端層簽章 *(oscSignatureMismatch)	風險	節點	錯誤

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
QoS 監控記憶體已滿 *(ocumQosMonitorMemoryMaxed)	風險	節點	錯誤
QoS 監控記憶體減少 *(ocumQosMonitorMemoryAbated)	事件	節點	資訊

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
節點已重新命名（不適用）	事件	節點	資訊

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
節點 IOPS 臨界閾值已突破（ocumNodeIopsIncident）	事件	節點	關鍵
節點 IOPS 警告臨界值已違反（ocumNodeIopsWarning）	風險	節點	警告
節點 MB/s 臨界閾值已突破（ocumNodeMbpsIncident）	事件	節點	關鍵
節點 MB/s 警告閾值已突破（ocumNodeMbpsWarning）	風險	節點	警告
節點延遲 ms/op 嚴重臨界值已突破（ocumNodeLatencyIncident）	事件	節點	關鍵
節點延遲 ms/op 警告臨界值已突破（ocumNodeLatencyWarning）	風險	節點	警告
節點效能容量使用率已超過臨界閾值（ocumNodePerfCapacityUsedIncident）	事件	節點	關鍵
節點效能容量使用量警告臨界值已違反（ocumNodePerfCapacityUsedWarning）	風險	節點	警告
節點效能容量已用 - 接管臨界閾值已突破（ocumNodePerfCapacityUsedTakeoverIncident）	事件	節點	關鍵
節點效能容量已使用 - 接管警告閾值已突破（ocumNodePerfCapacityUsedTakeoverWarning）	風險	節點	警告
節點使用率嚴重臨界值已突破（ocumNodeUtilizationIncident）	事件	節點	關鍵

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
節點使用率警告臨界值已突破（ocumNodeUtilizationWarning）	風險	節點	警告
節點 HA 配對過度使用臨界值已突破（ocumNodeHaPairOverUtilizedInformation）	事件	節點	資訊
節點磁碟碎片超過臨界值（ocumNodeDiskFragmentationWarning）	風險	節點	警告
效能容量使用量已超過臨界值（ocumNodeOverUtilizedWarning）	風險	節點	警告
節點動態臨界值已突破（ocumNodeDynamicEventWarning）	風險	節點	警告

影響領域：安全性

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
諮詢編號：NTAP-<*advisory ID*>（ocumx）	風險	節點	關鍵

了解 **Active IQ Unified Manager** 中的 **NVRAM** 電池事件

NVRAM 電池事件提供有關電池狀態的資訊，以便您監控潛力問題。事件依影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重程度。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
NVRAM 電池電量低（ocumEvtNvramBatteryLow）	風險	節點	警告
NVRAM 電池已放電（ocumEvtNvramBatteryDischarged）	風險	節點	錯誤
NVRAM 電池過度充電（ocumEvtNvramBatteryOverCharged）	事件	節點	關鍵

了解 **Active IQ Unified Manager** 中的連接埠事件

連接埠事件可提供您有關叢集連接埠的狀態，以便您可以監控連接埠上的變更或問題，例如連接埠是否已關閉。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
連接埠狀態已關閉（ocumEvtPortStatusDown）	事件	節點	關鍵

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
網路連接埠 MB/s 臨界閾值已突破（ocumNetworkPortMbpsIncident）	事件	連接埠	關鍵
網路連接埠 MB/s 警告閾值已突破（ocumNetworkPortMbpsWarning）	風險	連接埠	警告
FCP 連接埠 MB/s 臨界閾值已突破（ocumFcpPortMbpsIncident）	事件	連接埠	關鍵
FCP 連接埠 MB/s 警告臨界值已突破（ocumFcpPortMbpsWarning）	風險	連接埠	警告
網路連接埠利用率已突破臨界閾值（ocumNetworkPortUtilizationIncident）	事件	連接埠	關鍵
網路連接埠利用率警告閾值已突破（ocumNetworkPortUtilizationWarning）	風險	連接埠	警告
FCP 埠利用率已突破臨界閾值（ocumFcpPortUtilizationIncident）	事件	連接埠	關鍵
FCP 埠使用率警告臨界值已違反（ocumFcpPortUtilizationWarning）	風險	連接埠	警告

了解 **Active IQ Unified Manager** 中的電源供應器事件

電源供應器事件提供有關硬體狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重程度。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
一個或多個電源供應器故障（ocumEvtPowerSupplyOneOrMoreFailed）	事件	節點	關鍵

了解 **Active IQ Unified Manager** 中的保護事件

保護事件會告知您作業是否失敗或中止，以便您監控問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：保護

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
保護作業失敗（ocumEvtProtectionJobTaskFailed）	事件	Volume 或儲存設備服務	關鍵
保護工作已中止（ocumEvtProtectionJobAborted）	風險	Volume 或儲存設備服務	警告

了解 **Active IQ Unified Manager** 中的 **Qtree** 事件

Qtree 事件提供有關 qtree 容量以及檔案和磁碟限制的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
qtree 空間幾乎已滿（ocumEvtQtreeSpaceNearlyFull）	風險	Qtree	警告
Qtree 空間已滿（ocumEvtQtreeSpaceFull）	風險	Qtree	錯誤
Qtree 空間正常（ocumEvtQtreeSpaceThresholdOk）	事件	Qtree	資訊

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Qtree 檔案硬性限制已達上限（ocumEvtQtreeFilesHardLimitReached）	事件	Qtree	關鍵
Qtree 檔案軟性限制已超出（ocumEvtQtreeFilesSoftLimitBreached）	風險	Qtree	警告
qtree 空間硬限制已達到（ocumEvtQtreeSpaceHardLimitReached）	事件	Qtree	關鍵
Qtree 空間軟限制已突破（ocumEvtQtreeSpaceSoftLimitBreached）	風險	Qtree	警告

了解 **Active IQ Unified Manager** 中的服務處理器事件

服務處理器事件提供有關處理器狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和 trap 名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
服務處理器未設定（ocumEvtServiceProcessorNotConfigured）	風險	節點	警告
服務處理器離線（ocumEvtServiceProcessorOffline）	風險	節點	錯誤

了解 **Active IQ Unified Manager** 中的 **SnapMirror** 關係事件

SnapMirror 關係事件提供有關非同步和同步 SnapMirror 關係狀態的資訊，以便您可以監控潛力問題。非同步 SnapMirror 關係事件會針對儲存設備虛擬機器和 Volume 產生，而同步 SnapMirror 關係事件僅針對 Volume 關係產生。對於構成儲存設備虛擬機器災難恢復關係的 Volume，不會產生任何事件。事件按影響區域分組，並包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：保護

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

SnapMirror 關係事件是為受 Storage VM 災難恢復保護的 Storage VM 所產生，但不會為任何組成物件關係產生。

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
鏡像複寫不正常（ocumEvtSnapmirrorRelationshipUnhealthy）	風險	SnapMirror 關係	警告
鏡像複製已斷開（ocumEvtSnapmirrorRelationshipStateBrokenoff）	風險	SnapMirror 關係	錯誤
鏡像複寫初始化失敗（ocumEvtSnapmirrorRelationshipInitializeFailed）	風險	SnapMirror 關係	錯誤
鏡像複寫更新失敗（ocumEvtSnapmirrorRelationshipUpdateFailed）	風險	SnapMirror 關係	錯誤
鏡像複寫延遲錯誤（ocumEvtSnapMirrorRelationshipLagError）	風險	SnapMirror 關係	錯誤
鏡像複寫延遲警告（ocumEvtSnapMirrorRelationshipLagWarning）	風險	SnapMirror 關係	警告
鏡像複製重新同步失敗（ocumEvtSnapmirrorRelationshipResyncFailed）	風險	SnapMirror 關係	錯誤
同步複寫不同步 *（syncSnapmirrorRelationshipOutofsync）	風險	SnapMirror 關係	警告
同步複寫已恢復 *(syncSnapmirrorRelationshipInSync)	事件	SnapMirror 關係	資訊
同步複製自動重新同步失敗 *（syncSnapmirrorRelationshipAutoSyncRetryFailed）	風險	SnapMirror 關係	錯誤
Ontap Mediator 已新增至叢集中（snapmirrorMediatorAdded）	事件	叢集	資訊
Ontap Mediator 已從叢集中移除（snapmirrorMediatorRemoved）	事件	叢集	資訊
Ontap Mediator 無法從叢集存取（snapmirrorMediatorUnreachable）	風險	中介程式	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Ontap Mediator 無法從叢集存取（snapmirrorMediatorMisconfigured）	風險	中介程式	錯誤
Ontap Mediator 連線已重新建立，並已重新同步，可進行 SnapMirror 作用中同步（snapmirrorMediatorInQuorum）	事件	中介程式	資訊

了解 **Active IQ Unified Manager** 中的非同步鏡像和 **Vault** 關係事件

非同步鏡像和 Vault 關係事件提供有關非同步 SnapMirror 和 Vault 關係狀態的資訊，以便您可以監控潛力問題。非同步鏡像和 Vault 關係事件同時支援 Volume 和 Storage VM 保護關係。但僅 Vault 關係不支援 Storage VM 災難恢復。事件按影響區域分組，並包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：保護

針對受 Storage VM 災難恢復保護的 Storage VM，也會產生 SnapMirror 和 Vault 關係事件，但不會針對任何組成物件關係產生。

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
非同步鏡像和 Vault 不健康（ocumEvtMirrorVaultRelationshipUnhealthy）	風險	SnapMirror 關係	警告
非同步鏡像和保險庫已斷開（ocumEvtMirrorVaultRelationshipStateBrokenoff）	風險	SnapMirror 關係	錯誤
非同步鏡像和 Vault 初始化失敗（ocumEvtMirrorVaultRelationshipInitializeFailed）	風險	SnapMirror 關係	錯誤
非同步鏡像和保險庫更新失敗（ocumEvtMirrorVaultRelationshipUpdateFailed）	風險	SnapMirror 關係	錯誤
非同步鏡像和 Vault 延遲錯誤（ocumEvtMirrorVaultRelationshipLagError）	風險	SnapMirror 關係	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
非同步鏡像和 Vault 延遲警告（ocumEvtMirrorVaultRelationshipLagWarning）	風險	SnapMirror 關係	警告
非同步鏡像和 Vault 重新同步失敗（ocumEvtMirrorVaultRelationshipResyncFailed）	風險	SnapMirror 關係	錯誤

「SnapMirror 更新故障」事件由 Active IQ 入口網站（Config Advisor）引發。

了解 **Active IQ Unified Manager** 中的 **Snapshot** 快照技術事件

Snapshot 快照技術事件提供有關快照狀態的資訊，使您能夠監控快照是否存在潛力問題。這些事件按影響區域分組，並包含事件名稱、陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Snapshot 快照技術自動刪除已停用（不適用）	事件	磁碟區	資訊
Snapshot 快照技術自動刪除已啟用（不適用）	事件	磁碟區	資訊
Snapshot 快照技術自動刪除組態已修改（不適用）	事件	磁碟區	資訊

了解 **Active IQ Unified Manager** 中的 **SnapVault** 關係事件

SnapVault 關係事件提供有關 SnapVault 關係狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重程度。

影響區域：保護

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
非同步 Vault 不健全（ocumEvtSnapVaultRelationshipUnhealthy）	風險	SnapMirror 關係	警告
非同步 Vault 中斷（ocumEvtSnapVaultRelationshipStateBrokenoff）	風險	SnapMirror 關係	錯誤
非同步 Vault 初始化失敗（ocumEvtSnapVaultRelationshipInitializeFailed）	風險	SnapMirror 關係	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
非同步 Vault 更新失敗（ocumEvtSnapVaultRelationshipUpdateFailed）	風險	SnapMirror 關係	錯誤
非同步 Vault 延遲錯誤（ocumEvtSnapVaultRelationshipLagError）	風險	SnapMirror 關係	錯誤
非同步 Vault 延遲警告（ocumEvtSnapVaultRelationshipLagWarning）	風險	SnapMirror 關係	警告
非同步 Vault 重新同步失敗（ocumEvtSnapvaultRelationshipResyncFailed）	風險	SnapMirror 關係	錯誤

了解 **Active IQ Unified Manager** 中的儲存設備容錯移轉設定事件

儲存設備容錯移轉（SFO）設定事件提供有關儲存設備容錯移轉是否已停用或未設定的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重性。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
儲存設備故障轉移互連一或多個連結中斷（ocumEvtSfoInterconnectOneOrMoreLinksDown）	風險	節點	警告
儲存設備故障轉移已停用（ocumEvtSfoSettingsDisabled）	風險	節點	錯誤
未設定儲存設備故障轉移（ocumEvtSfoSettingsNotConfigured）	風險	節點	錯誤
儲存設備故障轉移狀態 - 接管（ocumEvtSfoStateTakeover）	風險	節點	警告
儲存設備故障轉移狀態 - 部分交還（ocumEvtSfoStatePartialGiveback）	風險	節點	錯誤
儲存故障轉移節點狀態已關閉（ocumEvtSfoNodeStatusDown）	風險	節點	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
無法進行儲存設備故障轉移接管（ocumEvtSfoTakeoverNotPossible）	風險	節點	錯誤

了解 **Active IQ Unified Manager** 中的儲存設備服務事件

儲存設備服務事件提供有關儲存設備服務的建立和訂閱資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
儲存設備服務已建立（不適用）	事件	儲存服務	資訊
已訂閱儲存服務（不適用）	事件	儲存服務	資訊
儲存服務已取消訂閱（不適用）	事件	儲存服務	資訊

影響區域：保護

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
意外刪除託管的 SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	風險	儲存服務	警告
儲存服務成員 Volume 意外刪除（ocumEvtStorageServiceUnexpectedVolumeDeletion）	事件	儲存服務	關鍵

了解 **Active IQ Unified Manager** 中的儲存設備機櫃事件

儲存設備機櫃事件會告知您儲存設備機櫃是否有異常，以便您監控潛力問題。事件依影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重程度。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
異常電壓範圍（ocumEvtShelfVoltageAbnormal）	風險	儲存機櫃	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
異常電流範圍（ocumEvtShelfCurrentAbnormal）	風險	儲存機櫃	警告
異常溫度（ocumEvtShelfTemperatureAbnormal）	風險	儲存機櫃	警告

了解 **Active IQ Unified Manager** 中的儲存 **VM** 事件

Storage VM （儲存設備虛擬機器，也稱為 SVM）事件提供有關 Storage VM （SVM）狀態的資訊，以便您可以監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重性。

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
儲存虛擬機器 CIFS 服務已關閉（ocumEvtVserverCifsServiceStatusDown）	事件	SVM	關鍵
SVM CIFS 服務未設定（不適用）	事件	SVM	資訊
嘗試連線不存在的 CIFS 共用 *（nbladeCifsNoPrivShare）	事件	SVM	關鍵
CIFS NetBIOS 名稱衝突 *(nbladeCifsNbNameConflict)	風險	SVM	錯誤
CIFS 卷影複製作業失敗 *（cifsShadowCopyFailure）	風險	SVM	錯誤
多個 CIFS 連線 *（nbladeCifsManyAuths）	風險	SVM	錯誤
CIFS 連線數超過上限 *（nbladeCifsMaxOpenSameFile）	風險	SVM	錯誤
每個使用者的 CIFS 連線數已超過最大值 *(nbladeCifsMaxSessPerUsrConn)	風險	SVM	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
SVM FC/FCoE 服務中斷（ocumEvtVserverFcServiceStatusDown）	事件	SVM	關鍵
SVM iSCSI 服務已關閉（ocumEvtVserverIscsiServiceStatusDown）	事件	SVM	關鍵
儲存 VM NFS 服務已關閉（ocumEvtVserverNfsServiceStatusDown）	事件	SVM	關鍵
SVM FC/FCoE 服務未設定（不適用）	事件	SVM	資訊
SVM iSCSI 服務未設定（不適用）	事件	SVM	資訊
SVM NFS 服務未設定（不適用）	事件	SVM	資訊
儲存 VM 已停止（ocumEvtVserverDown）	風險	SVM	警告
AV 伺服器繁忙，無法接受新的掃描請求 *(nbladeVscanConnBackPressure)	風險	SVM	錯誤
病毒掃描無 AV Server 連線 *（nbladeVscanNoScannerConn）	事件	SVM	關鍵
未註冊任何 AV 伺服器 *（nbladeVscanNoRegdScanner）	風險	SVM	錯誤
無回應的 AV 伺服器連線 *（nbladeVscanConnInactive）	事件	SVM	資訊
未經授權的使用者嘗試存取 AV 伺服器 *（nbladeVscanBadUserPrivAccess）	風險	SVM	錯誤
防毒伺服器發現病毒 *(nbladeVscanVirusDetected)	風險	SVM	錯誤

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
已發現 SVM（不適用）	事件	SVM	資訊

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
SVM 已刪除（不適用）	事件	叢集	資訊
SVM 已重新命名（不適用）	事件	SVM	資訊

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
SVM IOPS 臨界閾值已突破（ocumSvmIopsIncident）	事件	SVM	關鍵
SVM IOPS 警告閾值已突破（ocumSvmIopsWarning）	風險	SVM	警告
SVM MB/s 臨界閾值已突破（ocumSvmMbpsIncident）	事件	SVM	關鍵
SVM MB/s 警告臨界值已超出（ocumSvmMbpsWarning）	風險	SVM	警告
SVM 延遲臨界閾值已違反（ocumSvmLatencyIncident）	事件	SVM	關鍵
SVM 延遲警告臨界值已違反（ocumSvmLatencyWarning）	風險	SVM	警告

影響領域：安全性

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
稽核日誌已停用（ocumVserverAuditLogDisabled）	風險	SVM	警告
登入橫幅已停用（ocumVserverLoginBannerDisabled）	風險	SVM	警告
SSH 正在使用不安全的加密演算法（ocumVserverSSHInsecure）	風險	SVM	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
登入橫幅已變更（ocumVserverLoginBannerChanged）	風險	SVM	警告
儲存虛擬機器反勒索軟體監控已停用（antiRansomwareSvmStateDisabled）	風險	SVM	警告
儲存虛擬機器反勒索軟體監控已啟用（學習模式）（antiRansomwareSvmStateDryrun）	事件	SVM	資訊
適用於反勒索軟體監控的儲存虛擬機器（學習模式）（ocumEvtSvmArwCandidate）	事件	SVM	資訊

了解 **Active IQ Unified Manager** 中的使用者和群組配額事件

使用者和群組配額事件提供有關使用者和使用者群組配額容量以及檔案和磁碟限制的資訊，以便您監控潛力問題。事件按影響區域分組，包括事件和設陷名稱、影響層級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
使用者或群組配額磁碟空間軟限制已超出（ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached）	風險	使用者或群組配額	警告
使用者或群組配額磁碟空間已達到硬性限制（ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached）	事件	使用者或群組配額	關鍵
使用者或群組配額檔案數軟限制已超出（ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached）	風險	使用者或群組配額	警告
使用者或群組配額檔案數已達到硬性限制（ocumEvtUserOrGroupQuotaFileCountHardLimitReached）	事件	使用者或群組配額	關鍵

了解 **Active IQ Unified Manager** 中的 **Volume** 事件

Volume 事件提供有關 Volume 狀態的資訊，使您能夠監控潛力問題。這些事件按影響區域分組，並包含事件名稱、陷阱名稱、影響層級、來源類型和嚴重性。

星號（*）表示已轉換為 Unified Manager 事件的 EMS 事件。

影響區域：可用度

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 受限（ocumEvtVolumeRestricted）	風險	磁碟區	警告
Volume 離線（ocumEvtVolumeOffline）	事件	磁碟區	關鍵
Volume 部分可用（ocumEvtVolumePartiallyAvailable）	風險	磁碟區	錯誤
Volume 已卸載（不適用）	事件	磁碟區	資訊
Volume 已掛載（不適用）	事件	磁碟區	資訊
Volume 已重新掛載（不適用）	事件	磁碟區	資訊
Volume 接合路徑未啟動（ocumEvtVolumeJunctionPathInactive）	風險	磁碟區	警告
已啟用 Volume 自動調整大小（不適用）	事件	磁碟區	資訊
Volume 自動調整-已停用（不適用）	事件	磁碟區	資訊
Volume 自動調整最大容量修改（不適用）	事件	磁碟區	資訊
Volume 自動調整增量大小已修改（不適用）	事件	磁碟區	資訊

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
精簡配置 Volume 空間面臨風險（ocumThinProvisionVolumeSpaceAtRisk）	風險	磁碟區	警告
Volume 效率作業錯誤（ocumEvtVolumeEfficiencyOperationError）	風險	磁碟區	錯誤

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 空間已滿（ocumEvtVolumeFull）	風險	磁碟區	錯誤
Volume 空間幾乎已滿（ocumEvtVolumeNearlyFull）	風險	磁碟區	警告
Volume 邏輯空間已滿 *（volumeLogicalSpaceFull）	風險	磁碟區	錯誤
Volume 邏輯空間幾乎已滿 *(volumeLogicalSpaceNearlyFull)	風險	磁碟區	警告
Volume 邏輯空間正常 *（volumeLogicalSpaceAllOK）	事件	磁碟區	資訊
Volume Snapshot 快照技術預留空間已滿（ocumEvtSnapshotFull）	風險	磁碟區	警告
Snapshot 快照技術副本過多（ocumEvtSnapshotTooMany）	風險	磁碟區	錯誤
Volume Qtree 配額超額分配（ocumEvtVolumeQtreeQuotaOvercommitted）	風險	磁碟區	錯誤
Volume Qtree 配額幾乎超額分配（ocumEvtVolumeQtreeQuotaAlmostOvercommitted）	風險	磁碟區	警告
Volume 成長率異常（ocumEvtVolumeGrowthRateAbnormal）	風險	磁碟區	警告
Volume 距離磁碟空間耗盡的天數（ocumEvtVolumeDaysUntilFullSoon）	風險	磁碟區	錯誤
Volume 空間保證已停用（不適用）	事件	磁碟區	資訊
Volume 空間保證已啟用（不適用）	事件	磁碟區	資訊
Volume 空間保證已修改（不適用）	事件	磁碟區	資訊

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume Snapshot 快照技術儲備量滿載前剩餘天數（ocumEvtVolumeSnapshotReserveDaysUntilFullSoon）	風險	磁碟區	錯誤
FlexGroup 成員發生空間問題 *（flexGroupConstituentsHaveSpaceIssues）	風險	磁碟區	錯誤
FlexGroup 成員空間狀態全部正常 *(flexGroupConstituentsSpaceStatusAllOK)	事件	磁碟區	資訊
FlexGroup 成員存在 Inode 問題 *（flexGroupConstituentsHaveInodesIssues）	風險	磁碟區	錯誤
FlexGroup 成員 Inode 狀態全部正常 *(flexGroupConstituentsInodesStatusAllOK)	事件	磁碟區	資訊
WAFL Volume AutoSize 失敗 *(waflVolAutoSizeFail)	風險	磁碟區	錯誤
WAFL Volume AutoSize 已完成 *（waflVolAutoSizeDone）	事件	磁碟區	資訊
FlexGroup Volume 使用率超過 80%*	事件	磁碟區	錯誤
FlexGroup Volume 利用率超過 90%*	事件	磁碟區	關鍵
Volume 儲存效率異常（ocumVolumeAbnormalStorageEfficiencyWarning）	風險	磁碟區	警告
Volume Snapshot 快照技術保留空間未充分利用（volumeSnaphotReserveUnderutilizedWarning）	事件	磁碟區	警告
Volume Snapshot 快照技術保留空間未充分利用（volumeSnaphotReserveUnderutilizedCleared）	事件	磁碟區	警告

影響區域：組態

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 已重新命名（不適用）	事件	磁碟區	資訊
已發現 Volume（不適用）	事件	磁碟區	資訊
Volume 已刪除（不適用）	事件	磁碟區	資訊

影響領域：效能

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
QoS Volume 最大 IOPS 警告閾值已突破（ocumQosVolumeMaxIopsWarning）	風險	磁碟區	警告
QoS Volume 最大 MB/s 警告閾值已超出（ocumQosVolumeMaxMbpsWarning）	風險	磁碟區	警告
QoS Volume 最大 IOPS/TB 警告閾值已突破（ocumQosVolumeMaxIopsPerTbWarning）	風險	磁碟區	警告
工作負載 Volume 延遲閾值已超出效能服務層級策略（ocumConformanceLatencyWarning）定義的範圍	風險	磁碟區	警告
Volume IOPS 嚴重臨界值已超出（ocumVolumeIopsIncident）	事件	磁碟區	關鍵
Volume IOPS 警告閾值已突破（ocumVolumeIopsWarning）	風險	磁碟區	警告
Volume MB/s 已突破臨界閾值（ocumVolumeMbpsIncident）	事件	磁碟區	關鍵
Volume MB/s 警告閾值已突破（ocumVolumeMbpsWarning ）	風險	磁碟區	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 延遲臨界閾值已突破（ocumVolumeLatencyIncident）	事件	磁碟區	關鍵
Volume 延遲警告臨界值已超出（ocumVolumeLatencyWarning）	風險	磁碟區	警告
Volume 快取未命中率嚴重臨界值已突破（ocumVolumeCacheMissRatioIncident）	事件	磁碟區	關鍵
Volume 快取遺漏率警告臨界值已超出（ocumVolumeCacheMissRatioWarning）	風險	磁碟區	警告
Volume 延遲和 IOPS 重大臨界值已違反（ocumVolumeLatencyIopsIncident）	事件	磁碟區	關鍵
Volume 延遲和 IOPS 警告臨界值已突破（ocumVolumeLatencyIopsWarning）	風險	磁碟區	警告
Volume 延遲和 MB/s 重大臨界值已違反（ocumVolumeLatencyMbpsIncident）	事件	磁碟區	關鍵
Volume 延遲和 MB/s 警告臨界值已超出（ocumVolumeLatencyMbpsWarning）	風險	磁碟區	警告
Volume 延遲和 Aggregate 效能容量使用率已超過嚴重臨界值（ocumVolumeLatencyAggregatePerfCapacityUsedIncident）	事件	磁碟區	關鍵
Volume 延遲和 Aggregate 效能容量已使用警告臨界值超出（ocumVolumeLatencyAggregatePerfCapacityUsedWarning）	風險	磁碟區	警告

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 延遲和 Aggregate 使用率嚴重臨界值已突破（ocumVolumeLatencyAggregateUtilizationIncident）	事件	磁碟區	關鍵
Volume 延遲與 Aggregate 使用率警告臨界值已違反（ocumVolumeLatencyAggregateUtilizationWarning）	風險	磁碟區	警告
Volume 延遲和節點效能容量使用率已超過嚴重臨界值（ocumVolumeLatencyNodePerfCapacityUsedIncident）	事件	磁碟區	關鍵
Volume 延遲和節點效能容量使用量警告臨界值已突破（ocumVolumeLatencyNodePerfCapacityUsedWarning）	風險	磁碟區	警告
Volume 延遲和節點效能容量使用情況 - 接管重大臨界值已突破（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident）	事件	磁碟區	關鍵
Volume 延遲與節點已使用的效能容量 - 已違反接管警告臨界值（ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning）	風險	磁碟區	警告
Volume 延遲和節點利用率重大臨界值已突破（ocumVolumeLatencyNodeUtilizationIncident）	事件	磁碟區	關鍵
Volume 延遲與節點使用率警告臨界值已突破（ocumVolumeLatencyNodeUtilizationWarning）	風險	磁碟區	警告

影響領域：安全性

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 反勒索軟體監控已啟用（作用中模式）（antiRansomwareVolumeStateEnabled）	事件	磁碟區	資訊
Volume 反勒索軟體監控已停用（antiRansomwareVolumeStateDisabled）	風險	磁碟區	警告
Volume 防勒索軟體監控已啟用（學習模式）（antiRansomwareVolumeStateDryrun）	事件	磁碟區	資訊
Volume 防勒索軟體監控已暫停（學習模式）（antiRansomwareVolumeStateDryrunPaused）	風險	磁碟區	警告
Volume 防勒索軟體監控已暫停（作用中模式）（antiRansomwareVolumeStateEnablePaused）	風險	磁碟區	警告
Volume 反勒索軟體監控正在停用（antiRansomwareVolumeStateDisableInProgress）	風險	磁碟區	警告
發現勒索軟體活動（callHomeRansomwareActivitySeen）	事件	磁碟區	關鍵
適用於反勒索軟體監控的 Volume（學習模式）（ocumEvtVolumeArwCandidate）	事件	磁碟區	資訊
適用於反勒索軟體監控的 Volume（作用中模式）（ocumVolumeSuitedForActiveAntiRansomwareDetection）	風險	磁碟區	警告
Volume 顯示頻繁的反勒索軟體警報（antiRansomwareFeatureNoisyVolume）	風險	磁碟區	警告

影響領域：資料保護

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 本機 Snapshot 快照技術保護不足（volumeLacksLocalProtectionWarning）	風險	磁碟區	警告
Volume 本機 Snapshot 快照技術保護不足（volumeLacksLocalProtectionCleared）	風險	磁碟區	警告

了解 **Active IQ Unified Manager** 中的 **Volume** 移動狀態事件

Volume 遷移狀態事件會告知您 Volume 遷移的狀態，以便您監控潛力問題。事件按影響區域分組，包含事件和陷阱名稱、影響層級、來源類型和嚴重性。

影響區域：容量

事件名稱（陷阱名稱）	影響層級	來源類型	嚴重程度
Volume 搬移狀態：進行中（不適用）	事件	磁碟區	資訊
Volume 移動狀態 - 失敗（ocumEvtVolumeMoveFailed）	風險	磁碟區	錯誤
Volume 遷移狀態：已完成（不適用）	事件	磁碟區	資訊
Volume 搬移 - 延遲切換（ocumEvtVolumeMoveCutoverDeferred）	風險	磁碟區	警告

事件視窗和對話方塊的描述

了解 **Active IQ Unified Manager** 中的「通知」頁面

您可以設定 Unified Manager 伺服器，使其在產生事件或將事件指派給使用者時傳送通知。您也可以設定通知機制。例如，通知可以透過電子郵件或 SNMP 陷阱傳送。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

電子郵件

此區域可讓您設定下列警示通知的電子郵件設定：

- 寄件者地址

  指定傳送警示通知的來源電子郵件地址。共享報告時，此值也會用作寄件者地址。如果「寄件者地址」已預先填入「ActiveIQUnifiedManager@localhost.com」，您應將其變更為實際有效的電子郵件地址，以確保所有電子郵件通知均能成功傳遞。

SMTP 伺服器

您可以在此處設定以下 SMTP 伺服器設定：

- 主機名稱或 **IP** 位址

  指定 SMTP 主機伺服器的主機名稱，該主機名稱用於向指定的收件者發送警報通知。

- 使用者名稱

  指定 SMTP 使用者名稱。僅當 SMTP 伺服器啟用 SMTPAUTH 時才需要 SMTP 使用者名稱。

- 密碼

  指定 SMTP 密碼。僅當 SMTP 伺服器啟用 SMTPAUTH 時才需要 SMTP 使用者名稱。

- 連接埠

  指定 SMTP 主機伺服器用於發送警報通知的連接埠。

  預設值為 25。

- 使用 **START/TLS**

  勾選此方塊可透過使用 TLS/SSL 協定（也稱為 start_tls 和 StartTLS）在 SMTP 伺服器和管理伺服器之間提供安全的通訊。

- 使用 **SSL**

  勾選此方塊可透過使用 SSL 協定在 SMTP 伺服器和管理伺服器之間提供安全的通訊。

SNMP

在此區域，您可以設定以下 SNMP 陷阱設定：

- 版本

  根據您所需的安全性類型，指定您要使用的 SNMP 版本。選項包括版本 1、版本 3、具備驗證的版本 3，以及具備驗證與加密的版本 3。預設值為版本 1。

- **Trap** 目的地主機

  指定接收管理伺服器傳送的 SNMP 陷阱的主機名稱或 IP 位址（IPv4 或 IPv6）。若要指定多個陷阱目標，請用逗號分隔每個主機。

  > ⓘ 所有其他 SNMP 設定（例如「版本」和「出站連接埠」）對於清單中的所有主機都必須相同。

- 傳出 **Trap** 連接埠

  指定 SNMP 伺服器用來接收管理伺服器所傳送之陷阱的連接埠。

  預設值為 162。

- 社群

  用於存取主機的社群字串。

- 引擎識別碼

  指定 SNMP 代理程式的唯一識別碼，並由管理伺服器自動產生。引擎 ID 可用於 SNMP 版本 3、具有驗證的 SNMP 版本 3，以及具有驗證和加密的 SNMP 版本 3。

- 使用者名稱

  指定 SNMP 使用者名稱。SNMP 版本 3、具有驗證的 SNMP 版本 3 以及具有驗證和加密的 SNMP 版本 3 均支援使用者名稱。

- 身份驗證協定

  指定用於驗證使用者的協定。協定選項包括 MD5 和 SHA。MD5 為預設值。驗證協定適用於具有驗證的 SNMP 版本 3 和具有驗證與加密的 SNMP 版本 3。

- 驗證密碼

  指定驗證使用者時所使用的密碼。SNMP 第 3 版（含驗證）和 SNMP 第 3 版（含驗證與加密）均提供驗證密碼。

- 隱私權通訊協定

  指定用於加密 SNMP 訊息的隱私協定。協定選項包括 AES 128 和 DES。預設值為 AES 128。隱私協定在啟用驗證和加密的 SNMP 版本 3 中可用。

- 隱私密碼

  指定使用隱私協定時的密碼。隱私權密碼適用於啟用驗證和加密的 SNMP 版本 3。

如需有關 SNMP 物件與陷阱的詳細資訊，您可以從 NetApp 支援網站下載 "Active IQ Unified Manager MIB"。

了解 **Active IQ Unified Manager** 中的事件管理清單頁面

事件管理清單頁面可讓您檢視目前事件及其屬性的清單。您可以執行確認、解決及指派事件等工作。您也可以為特定事件新增警示。

本頁面的資訊每 5 分鐘會自動重新整理一次，以確保顯示最新的事件。

篩選器元件

可讓您自訂事件清單中顯示的資訊。您可以使用下列元件來精簡所顯示的事件清單：

- 檢視選單，從預先定義的篩選選項清單中進行選擇。

  這包括所有作用中（新的和已確認的）事件、作用中效能事件、分配給我（登入使用者）的事件以及所有維護視窗期間產生的所有事件等項目。

- 搜尋窗格，可透過輸入完整或部分詞彙來精簡事件清單。

- 篩選按鈕可啟動篩選器窗格，讓您從每個可用的欄位和欄位屬性中進行選擇，以精簡事件清單。

命令按鈕

命令按鈕可讓您執行下列任務：

- 指派給

  您可以選擇事件的指定使用者。當您將事件指派給使用者時，該使用者的姓名和指派時間將會新增至所選事件的事件清單中。

  - 我

    將事件指派給目前登入的使用者。

  - 另一位使用者

    顯示「指定擁有者」對話方塊，讓您能夠將事件指派或重新指派給其他使用者。您也可以將所有權欄位留白來取消指派事件。

- 確認

  確認所選事件。

  當您確認事件時，您的使用者名稱和確認事件的時間會新增至所選事件的事件清單中。當您確認事件時，您將負責管理該事件。

  您無法確認資訊事件。

- 標記為已解決

  允許您將事件狀態變更為已解決。

  當您解決事件時，您的使用者名稱和解決事件的時間會加入所選事件的事件清單中。在您對事件採取修正行動後，必須將該事件標記為已解決。

- 新增提醒

  顯示「新增警示」對話框，可讓您為所選事件新增警示。

- 報告

  可讓您將目前事件檢視的詳細資訊匯出至逗號分隔值（.csv）檔案或 PDF 文件。

- 顯示/隱藏欄選擇器

  可讓您選擇要在頁面上顯示的欄，並選擇其顯示順序。

事件清單

顯示所有事件的詳細資料，並依觸發時間排序。

預設會顯示「所有作用中事件」檢視，以顯示過去七天內影響層級為「事件」或「風險」的新事件和已確認事件。

- 觸發時間

  事件產生的時間。

- 嚴重程度

  事件嚴重性：嚴重（）、錯誤（）、警告（）與資訊（）。

- 狀態

  事件狀態：新建、已確認、已解決或已過時。

- 影響層級

  事件影響層級：事故、風險、事件或升級。

- 影響區域

  事件影響範圍：可用度、容量、效能、保護、組態或安全性。

- 名稱

  事件名稱。您可以選擇名稱以顯示該事件的事件詳細資料頁面。

- 來源

  發生事件的物件名稱。您可以選擇該名稱以顯示該物件的健全狀況或效能詳細資料頁面。

  當共享的 QoS 原則發生違規時，此欄位僅顯示消耗 IOPS 或 MB/s 最多的工作負載物件。使用此原則的其他工作負載將顯示在「事件詳細資料」頁面中。

- 來源類型

  與事件關聯的物件類型（例如，Storage VM、磁碟區或 Qtree）。

- 指派給

  獲派事件的使用者名稱。

- 事件起源

  事件是源自「Active IQ Portal」還是直接源自「Active IQ Unified Manager」。

- 註解名稱

  指派給儲存設備物件的註解名稱。

- 備註

  為某個事件新增的附註數量。

- 未解決天數

  自事件最初產生以來的天數。

- 指定時間

  自事件指派給使用者以來所經過的時間。如果經過的時間超過一週，則會顯示事件指派給使用者的時間戳記。

- 確認者

  確認事件的使用者名稱。如果事件未確認，則此欄位為空白。

- 確認時間

  自事件確認以來經過的時間。如果經過的時間超過一週，則顯示事件確認的時間戳記。

- 解決者

  解決事件的使用者名稱。如果事件未解決，則此欄位為空白。

- 已解決時間

  自事件解決後所經過的時間。如果經過的時間超過一週，則會顯示事件解決時的時間戳記。

- 過時時間

  該事件狀態過時的時間點。

事件詳情頁面

了解 **Active IQ Unified Manager** 中的「事件詳細資料」頁面

在「事件詳細資料」頁面中，您可以檢視所選事件的詳細資訊，例如事件嚴重性、影響層級、影響區域和事件來源。您也可以檢視有關解決該問題之可能補救措施的其他資訊。

- 事件名稱

  事件名稱和事件最後一次出現的時間。

  對於非效能事件，當事件處於「新增」或「已確認」狀態時，最後看見的資訊為未知，因此會隱藏。

- 事件執行摘要

  事件的簡短執行摘要。

  在某些情況下，事件執行摘要中會提供觸發事件的原因。

- 發生競爭的元件

  對於動態效能事件，此部分會顯示代表叢集邏輯元件和實體元件的圖示。如果某個元件處於爭用狀態，其圖示會被圈起並以紅色醒目提示。

如需此處顯示之元件的執行摘要，請參閱 叢集元件及其可能發生爭用的原因。

事件資訊、系統診斷和建議行動部分將在其他主題中說明。

命令按鈕

命令按鈕可讓您執行下列任務：

- 附註圖示

  您可以新增或更新有關該事件的附註，並審查其他使用者留下的所有附註。

操作選單

- 指派給我

  將事件指派給您。

- 指派給其他人

  開啟「指派擁有者」對話方塊，您可以透過該對話方塊將事件指派或重新指派給其他使用者。

  當您將事件指派給使用者時，使用者的姓名和事件指派時間將會新增至所選事件的事件清單中。

  您也可以將所有權欄位留空來取消分配事件。

- 確認

  確認所選事件，以便您不再收到重複的警報通知。

  當您確認事件時，您的使用者名稱和確認事件的時間將會新增至所選事件的事件清單（確認者）中。確認事件後，您將負責管理該事件。

- 標記為已解決

  可讓您將事件狀態變更為「已解決」。

  當您解決事件時，您的使用者名稱以及解決事件的時間將會新增至所選事件的事件清單中 （Resolved By ）。針對事件採取修正行動後，您必須將事件標示為已解決。

- 新增提醒

  顯示「新增警報」對話方塊，讓您為選取的事件新增警報。

了解 **Active IQ Unified Manager** 中的「事件資訊」部分

您可以使用「事件詳細資料」頁面上的「事件資訊」區段來檢視所選事件的詳細資訊，例如事件嚴重性、影響層級、影響區域和事件來源。

不適用於該事件類型的欄位已被隱藏。您可以檢視以下事件詳情：

- 事件觸發時間

事件產生的時間。

- 狀態

  事件狀態：新建、已確認、已解決或已過時。

- 已過時的原因

  導致事件過時的行動，例如，問題已修復。

- 事件持續時間

  對於作用中（新發生且已確認）的事件，此時間是指從偵測到事件至最後一次分析事件之間的時間。對於已過時的事件，此時間是指從偵測到事件至事件解決之間的時間。

  此欄位會顯示在所有效能事件中，而對於其他事件類型，只有在事件解決或過時後才會顯示。

- 最後出現時間

  事件最後一次處於作用中的日期和時間。

  對於效能事件，此值可能會比事件觸發時間更新，因為只要事件處於作用中，每次收集到新的效能資料後，此欄位都會更新。對於其他類型的事件，當處於「新」或「已確認」狀態時，此內容不會更新，因此該欄位會被隱藏。

- 嚴重程度

  事件嚴重性：嚴重（）、錯誤（）、警告（）與資訊（）。

- 影響層級

  事件影響層級：事故、風險、事件或升級。

- 影響區域

  事件影響範圍：可用度、容量、效能、保護、組態或安全性。

- 來源

  發生事件的物件名稱。

  在檢視共享的 QoS 原則事件的詳細資訊時，此欄位中最多會列出消耗最多 IOPS 或 MBps 的三個工作負載物件。

  您可以點選來源名稱連結來顯示該物件的健全狀況或效能詳細資料頁面。

- 來源註解

  顯示與事件關聯的物件的註解名稱和值。

  此欄位僅針對叢集、SVM 和 Volume 上的健全狀況事件顯示。

- 來源群組

顯示受影響物件所屬的所有群組的名稱。

此欄位僅針對叢集、SVM 和 Volume 上的健全狀況事件顯示。

- 來源類型

  與事件關聯的物件類型（例如 SVM、Volume 或 Qtree）。

- 叢集上

  事件發生的叢集名稱。

  您可以按一下叢集名稱連結，顯示該叢集的健全狀況或效能詳細資訊頁面。

- 受影響物件數量

  受事件影響的物件數量。

  您可以按一下物件連結來顯示詳細目錄頁面，其中包含目前受此事件影響的物件。

  此欄位僅針對效能事件顯示。

- 受影響的 **Volume**

  受此事件影響的 Volume 數量。

  此欄位僅針對節點或 Aggregate 上的效能事件顯示。

- 觸發原則

  發布該事件的臨界值原則的名稱。

  您可以將滑鼠懸停在原則名稱上，查看臨界值原則的詳細資訊。對於具調適能力的 QoS 原則，也會顯示已定義的原則、區塊大小和分配類型（已分配空間或已使用空間）。

  此欄位僅針對效能事件顯示。

- 規則 **ID**

  對於 Active IQ 平台事件，這是觸發產生該事件的規則編號。

- 確認者

  確認事件的人員姓名以及確認事件的時間。

- 解決者

  事件解決者的姓名以及事件解決的時間。

- 分配給

  負責此次事件的人員姓名。

- 提醒設定

  顯示下列有關警報的資訊：

  - 如果所選事件沒有關聯的警報，則會顯示 新增警報 連結。

    按一下連結即可開啟「新增警報」對話方塊。

  - 如果有一個警報與選定的事件相關聯，則會顯示警報名稱。

    您可以點擊連結開啟「編輯警示」對話方塊。

  - 如果與所選事件關聯的警報不只一個，則會顯示警報的數量。

    您可以點擊連結開啟「警報設定」頁面，檢視有關這些警報的更多詳細資訊。

  已停用的警報不會顯示。

- 最後傳送的通知

  最近一次警報通知的發送日期和時間。

- 發送人

  發送警報通知所使用的機制：電子郵件或 SNMP trap。

- 上次指令碼執行

  警報產生時執行的指令碼名稱。

了解 **Active IQ Unified Manager** 中的建議操作

事件詳細資料頁面的「建議行動」區段提供了事件的可能原因，並建議了一些行動，以便您嘗試自行解決事件。這些建議行動是根據事件類型或超出的臨界值類型所自訂的。

此區域僅針對某些類型的事件顯示。

在某些情況下，頁面上會提供 **Help** 連結，其中包含許多建議行動的其他資訊，包括執行特定行動的指示。某些行動可能涉及使用 Unified Manager 、 ONTAP System Manager 、 OnCommand Workflow Automation 、 ONTAP CLI 命令或這些工具的組合。

您應將此處建議的行動僅視為解決此事件的指引。您為解決此事件所採取的行動，應根據您環境的背景而定。

如果要更詳細地分析物件和事件，請按一下 分析工作負載 按鈕以顯示工作負載分析頁面。

Unified Manager 可以徹底診斷某些事件並提供單一解決方案。如果解決方案可用，則會顯示 **Fix It** 按鈕。按一下此按鈕，讓 Unified Manager 修復導致該事件的問題。

對於 Active IQ 平台事件，本部分可能包含 NetApp 知識庫文章的連結（如果可用），該文章描述了問題及可能的解決方案。在沒有外部網路存取的站點，知識庫文章的 PDF 檔案將在本機開啟；該 PDF 檔案包含在您手動下載到 Unified Manager 執行個體的規則檔案中。

事件詳細資料頁面的「系統診斷」部分提供有助於診斷可能導致該事件之問題的資訊。

此區域僅針對部分事件顯示。

某些效能事件會提供與觸發的特定事件相關的圖表。通常這包括過去十天的 IOPS 或 MBps 圖表以及延遲圖表。透過這種排列方式，您可以在事件作用中時，查看哪些儲存設備元件對延遲的影響最大，或受延遲的影響最大。

對於動態效能事件，將顯示以下圖表：

- 工作負載延遲 - 顯示發生爭用的元件上，排名最高的受害者、惡霸或鯊魚工作負載的延遲歷史記錄。
- 工作負載活動 - 顯示有關爭用叢集元件的工作負載使用情況的詳細資訊。
- 資源活動 - 顯示發生爭用的叢集元件的歷史效能統計資料。

當某些叢集元件發生爭用時，會顯示其他圖表。

其他事件提供系統正在對儲存設備物件執行的分析類型的簡要執行摘要。在某些情況下，可能會出現一行或多行；對於分析多個效能計數器的系統定義效能原則，每行對應一個已分析的元件。在這種情況下，診斷結果旁邊會顯示綠色或紅色圖示，以指示該特定診斷中是否發現了問題。

了解 **Active IQ Unified Manager** 中的「事件設定」頁面

「事件設定」頁面會顯示已停用事件的清單，並提供相關物件類型和事件嚴重性等資訊。您也可以執行全域停用或啟用事件等工作。

只有擁有應用程式管理員或儲存設備管理員角色的使用者才能存取此頁面。

命令按鈕

命令按鈕可讓您對選定的事件執行以下操作：

- 停用

  開啟「停用事件」對話框，您可以使用該對話框停用事件。

- 啟用

  啟用您之前選擇停用的所選事件。

- 上傳規則

  啟動「上傳規則」對話方塊，讓沒有外部網路存取的網站能夠手動將 Active IQ 規則檔案上傳至 Unified Manager。這些規則會針對叢集 AutoSupport 訊息執行，以產生 Active IQ 平台所定義的系統組態、佈線、最佳實務做法和可用度事件。

- 訂閱 **EMS** 事件

  啟動「訂閱 EMS 事件」對話方塊，讓您能夠訂閱以接收來自您正在監控之叢集的特定事件管理系統（EMS）事件。EMS 會收集有關叢集上發生之事件的資訊。當收到已訂閱之 EMS 事件的通知時，系統會產生具有適當嚴重性的 Unified Manager 事件。

清單檢視

清單檢視以表格形式顯示已停用事件的相關資訊。您可以使用欄篩選器自訂顯示的資料。

- 事件

  顯示已停用事件的名稱。

- 嚴重程度

  顯示事件的嚴重程度。嚴重程度分為：嚴重、錯誤、警告或訊息。

- 來源類型

  顯示產生事件的來源類型。

在 **Active IQ Unified Manager** 中停用「事件」對話方塊

「停用事件」對話方塊顯示可停用事件的事件類型清單。您可以根據特定嚴重程度或一組事件停用事件類型的事件。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

事件屬性區域

「事件屬性」區域指定下列事件屬性：

- 事件嚴重程度

  允許您根據嚴重性類別選擇事件，嚴重性類別可以是關鍵、錯誤、警告或資訊。

- 事件名稱包含

  允許您篩選名稱包含指定字元的事件。

- 相符事件

  顯示與事件嚴重性類別和您指定的字串相符的事件清單。

- 停用事件

  顯示您已選擇要停用的事件清單。

  事件的嚴重程度也會與事件名稱一起顯示。

命令按鈕

透過命令按鈕，您可以對選定的事件執行以下操作：

- 儲存並結案

  停用該事件類型並關閉對話方塊。

- 取消

  放棄變更並關閉對話方塊。

管理警報

了解 **Active IQ Unified Manager** 中的警示

儘管事件會持續發生，但 Unified Manager 僅在事件符合指定的篩選條件時才會產生警報。您可以選擇要產生警報的事件，例如，當空間超過臨界值或物件離線時。您也可以將警報與觸發警報時執行的指令碼關聯起來。

篩選條件包括物件類別、名稱或事件嚴重性。

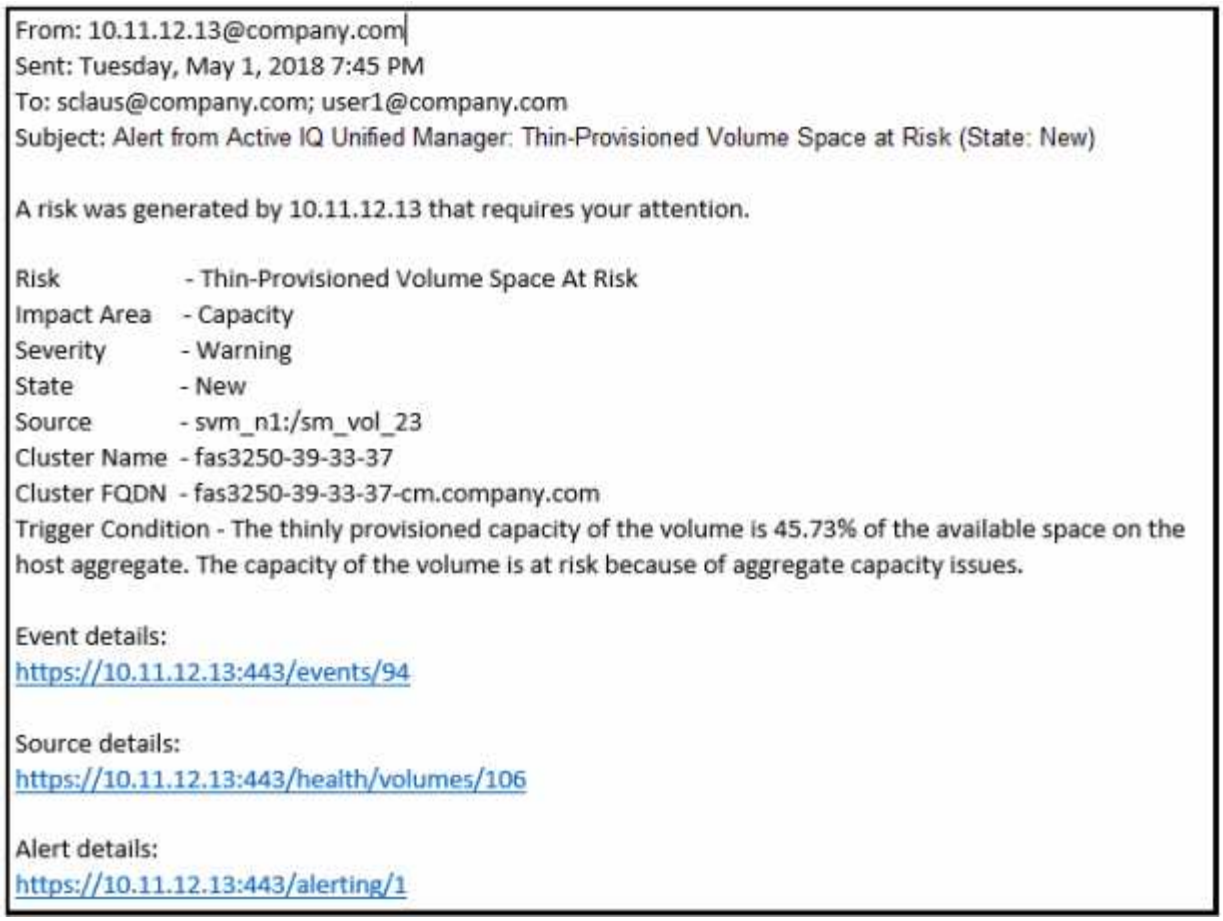
Active IQ Unified Manager 警報電子郵件中包含的資訊

Unified Manager 警示電子郵件會提供事件類型、事件嚴重程度、遭違反並導致事件的原則或臨界值名稱，以及事件的執行摘要。電子郵件訊息也會為每個事件提供超連結，讓您可以在 UI 中檢視該事件的詳細資料頁面。

系統會傳送提醒郵件給所有訂閱接收提醒的使用者。

如果在收集期間效能計數器或容量值發生大幅變化，可能會導致同一個臨界值原則同時觸發關鍵和警告事件。在這種情況下，您可能會收到一封警告事件的電子郵件和一封關鍵事件的電子郵件。這是因為 Unified Manager 允許您分別訂閱接收警告和關鍵臨界值超限的警報。

以下是一封範例警報郵件：


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

新增警示

在 **Active IQ Unified Manager** 中新增警報

您可以設定警報，以便在產生特定事件時收到通知。您可以為單一資源、一組資源或特定嚴重性類別的事件設定警報。您可以指定接收通知的頻率，並將指令碼關聯至警報。

開始之前

- 您必須設定通知設定，例如使用者電子郵件地址、SMTP 伺服器和 SNMP trap 主機，才能使 Active IQ Unified Manager 伺服器使用這些設定，在產生事件時傳送通知給使用者。
- 您必須知道要觸發警報的資源和事件，以及要通知的使用者的使用者名稱或電子郵件地址。
- 如果您希望根據事件執行指令碼，則必須使用「指令碼」頁面將指令碼新增至 Unified Manager。
- 您必須擁有應用程式系統管理員或儲存系統管理員角色。

除了可以按照此處所述從「警報設定」頁面建立警報外，您還可以在收到事件後直接從「事件詳情」頁面建立警報。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面中，按一下 新增。
3. 在 新增警報 對話方塊中，按一下 名稱，然後輸入警報的名稱和執行摘要。

4. 按一下 資源，然後選擇要包含在警報中或從警報中排除的資源。

   您可以透過在 名稱包含 欄位中指定字串來設定篩選條件，從而選擇一組資源。根據您指定的字串，可用資源清單將僅顯示符合篩選規則的資源。您指定的字串區分大小寫。

   如果資源同時符合您指定的包含規則和排除規則，則排除規則優先於包含規則，並且不會為與排除資源相關的事件產生警報。

5. 按一下 事件，然後根據事件名稱或事件嚴重性類別選擇要觸發警報的事件。

   若要選擇多個事件，請在選擇時按住 Ctrl 鍵。

6. 按一下 **Actions** ，選擇要通知的使用者，選擇通知頻率，選擇是否將 SNMP trap 傳送至 trap 接收器，並指派在產生警報時要執行的指令碼。

   如果您修改了為使用者指定的電子郵件地址，並重新開啟警示以進行編輯，則「名稱」欄位會顯示為空白，因為修改後的電子郵件地址不再對應至先前選取的使用者。此外，如果您從「使用者」頁面修改了所選使用者的電子郵件地址，則修改後的電子郵件地址不會為所選使用者更新。

   您也可以選擇透過 SNMP 陷阱通知使用者。

7. 按一下 **Save** 。

新增警報的範例

本範例展示如何建立滿足以下要求的警報：

- 警報名稱：HealthTest
- 資源：包括名稱中包含「abc」的所有磁碟區，且不包括名稱中包含「xyz」的所有磁碟區
- 事件：包括所有關鍵健全狀況事件
- 操作：包括「sample@domain.com」、一個「Test」指令碼，並且需要每 15 分鐘通知使用者一次

在「新增警報」對話方塊中執行以下步驟：

1. 點擊 名稱，然後在 警報名稱 欄位中輸入 **`HealthTest`**。
2. 按一下 資源 ，然後在 Include 索引標籤中，從下拉清單中選取 磁碟區 。
   a. 在 名稱包含 欄位中輸入 **`abc`**，以顯示名稱包含 "abc" 的磁碟區。
   b. 從「可用資源」區域選取 **<<All Volumes whose name contains 'abc'>>**，並將其移至「已選資源」區域。
   c. 按一下 排除，在 名稱包含 欄位中輸入 **`xyz`**，然後按一下 新增。
3. 按一下 事件，然後在「事件嚴重性」欄位中選擇 關鍵。
4. 從相符事件區域中選取 所有關鍵事件，並將其移至選取的事件區域。
5. 按一下 動作 ，然後在「通知這些使用者」欄位中輸入 **`sample@domain.com`** 。
6. 選擇 每 **15** 分鐘提醒一次 即可每 15 分鐘通知使用者一次。

您可以設定警報，使其在指定時間內重複向收件人發送通知。您應該決定警報的事件通知開始作用中的時間。

7. 在「選擇要執行的指令碼」功能表中，選擇 **Test** 指令碼。
8. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中新增警報的指南

您可以根據資源（例如叢集、節點、彙總或 Volume）以及特定嚴重性類別的事件新增警報。最佳實務做法是，在新增物件所屬的叢集之後，再為任何關鍵物件新增警報。

您可以參考以下準則和注意事項來建立警報，從而有效管理系統：

- 警報執行摘要

  您應該為警報提供執行摘要，以便有效地追蹤警報。

- 資源

  您需要決定哪些實體或邏輯資源需要發出警報。您可以根據需要包含或排除資源。例如，如果您想要透過設定警報來密切監控您的彙總，則必須從資源清單中選擇所需的彙總。

  如果您選擇資源類別，例如 **<<All User or Group Quotas>>**，那麼您將收到該類別中所有物件的警報。

  選擇叢集作為資源並不會自動選擇該叢集內的儲存設備物件。例如，如果您為所有叢集的所有關鍵事件建立警報，則只會收到叢集關鍵事件的警報。您不會收到節點、彙總等關鍵事件的警報。

- 事件嚴重性

  您應該決定特定嚴重性類別（關鍵、錯誤、警告）的事件是否應觸發警報，如果是，則應觸發哪種嚴重性類別。

- 選取的事件

  如果根據產生的事件類型新增警報，則應決定哪些事件需要警報。

  如果您選擇事件嚴重性，但沒有選擇任何單一事件（如果您將「已選事件」列留空），則您將收到該類別中所有事件的警報。

- 動作

  您必須提供接收通知的使用者的使用者名稱和電子郵件地址。您也可以指定 SNMP 陷阱作為通知方式。您可以將指令碼與警報關聯，以便在產生警報時執行指令碼。

- 通知頻率

  您可以設定警報，使其在指定時間內重複向收件人發送通知。您需要確定警報事件通知的作用中時間。如果您希望事件通知持續發送直至事件被確認，則需要確定通知的重複頻率。

- 執行指令碼

您可以將指令碼與警報建立關聯。產生警報時，即會執行您的指令碼。

在 **Active IQ Unified Manager** 中新增效能事件警報

您可以像設定 Unified Manager 接收的任何其他事件一樣，為個別效能事件設定警報。此外，如果您希望將所有效能事件一視同仁，並將電子郵件傳送給同一個人，您可以建立單一警報，以便在觸發任何關鍵或警告效能事件時通知您。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

以下範例顯示如何為所有關鍵延遲、IOPS 和 MBps 事件建立事件。您可以使用相同的方法從所有效能計數器中選擇事件，以及所有警告事件。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面中，按一下 新增。
3. 在 新增警報 對話方塊中，按一下 名稱，然後輸入警報的名稱和執行摘要。
4. 請勿在「資源」頁面上選擇任何資源。

   由於未選取任何資源，因此警報會套用至收到這些事件的所有叢集、集合體、磁碟區等。

5. 按一下 事件 並執行下列動作：
   a. 在事件嚴重性清單中，選擇 關鍵。
   b. 在「事件名稱包含」欄位中，輸入 **`latency`**，然後按一下箭頭選擇所有符合的事件。
   c. 在「事件名稱包含」欄位中，輸入`*iops*`，然後按一下箭頭選擇所有符合的事件。
   d. 在「事件名稱包含」欄位中，輸入 **`mbps`**，然後按一下箭頭選擇所有符合的事件。
6. 按一下 動作 ，然後在 警示這些使用者 欄位中選取將收到警示電子郵件的使用者名稱。
7. 在本頁上設定發出 SNMP 陷阱和執行指令碼的任何其他選項。
8. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中測試警報

您可以測試警報以驗證設定是否正確。當事件觸發時，會產生警報，並將警報電子郵件傳送給已設定的收件者。您可以使用測試警報來驗證通知是否已傳送，以及指令碼是否已執行。

開始之前

- 您必須已設定通知設定，例如收件者的電子郵件地址、SMTP 伺服器和 SNMP 設陷。

  Unified Manager 伺服器可以使用這些設定，在產生事件時向使用者傳送通知。

- 您必須已指派指令碼並設定該指令碼，以便在產生警報時執行。
- 您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面中，選擇您要測試的警報，然後按一下 測試。

   系統會傳送測試警報郵件給您在建立警報時指定的電子郵件地址。

停用 **Active IQ Unified Manager** 中已解決與已過時事件的警報

對於所有已配置為發送警報的事件，當這些事件經歷所有可用狀態（New、Resolved 和 Obsolete）時，系統都會發送警報訊息。如果您不希望接收事件進入 Resolved 和 Obsolete 狀態時的警報，您可以設定全域設定來抑制這些警報。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

預設情況下，事件進入「已解決」和「已過時」狀態時不會發送警報。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面中，使用 已解決且已過時事件的警報 項目旁的滑桿控制執行下列其中一項動作：

若要.....	這樣做.....
事件解決或過時後，停止發送警報	將滑桿控制向左移動
當事件解決或過時，開始發送警報	將滑桿控制向右移動

將災難恢復目的地 **Volume** 從 **Active IQ Unified Manager** 的警報產生中排除

設定 Volume 警報時，您可以在「警報」對話方塊中指定字串來識別 Volume 或 Volume 群組。但是，如果您已為 SVM 設定了災難恢復，則來源和目的地 Volume 的名稱相同，因此您將收到兩個 Volume 的警報。

開始之前

您必須擁有應用程式系統管理員或儲存系統管理員角色。

您可以透過排除具有目的地 SVM 名稱的 Volume 來停用災難恢復目的地 Volume 的警報。這是因為 Volume 事件的識別碼包含 SVM 名稱和 Volume 名稱，格式為「<svm_name>:/<volume_name>」。

下列範例顯示如何為主 SVM「vs1」上的 Volume「vol1」建立警報，但排除在 SVM「vs1-dr」上同名 Volume 產生警報。

在「新增警報」對話方塊中執行以下步驟：

步驟

1. 按一下 名稱 並輸入警報的名稱和執行摘要。
2. 按一下 資源，然後選取 包含 索引標籤。

a. 從下拉清單中選擇 **Volume**，然後在 名稱包含 欄位中輸入 **`vol1`**，以顯示名稱包含 "vol1" 的 Volume。

b. 從 可用資源 區域選取 **<<All Volumes whose name contains 'vol1'>>**，並將其移至 已選取資源 區域。

3. 選取 排除 索引標籤，選取 **Volume**，在 名稱包含 欄位中輸入 **`vs1-dr`**，然後按一下 新增。

   這會排除為 SVM "vs1-dr" 上的 Volume "vol1" 產生警報。

4. 按一下 **Events** ，然後選取要套用至 Volume 或多個 Volume 的事件。
5. 按一下 動作 ，然後在 警示這些使用者 欄位中選取將收到警示電子郵件的使用者名稱。
6. 在此頁面上設定發出 SNMP 陷阱和執行指令碼的任何其他選項，然後按一下 儲存。

在 **Active IQ Unified Manager** 中查看警報

您可以在「警報設定」頁面檢視針對各種事件所建立的警報清單。您還可以檢視警報屬性，例如警報執行摘要、通知方法和頻率、觸發警報的事件、警報的電子郵件收件人以及受影響的資源，例如叢集、彙總和 Volume。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。

   警報清單顯示在「警報設定」頁面中。

在 **Active IQ Unified Manager** 中編輯警報

您可以編輯警報屬性，例如警報關聯的資源、事件、收件者、通知選項、通知頻率和關聯的指令碼。

開始之前

您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在*警報設定*頁面中，選擇要編輯的警報，然後按一下*編輯*。
3. 在 編輯警報 對話方塊中，視需要編輯名稱、資源、事件和行動區段。

   您可以變更或移除與警報關聯的指令碼。

4. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中刪除警報

您可以刪除不再需要的警報。例如，當 Unified Manager 不再監控某個資源時，您可以刪

除為該資源建立的警報。

開始之前

您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在 警報設定 頁面上，選擇要刪除的警報，然後按一下 刪除。
3. 點擊 是 確認刪除請求。

警告視窗和對話方塊的說明

了解 **Active IQ Unified Manager** 中的「警報設定」頁面

「警報設定」頁面顯示警報列表，並提供有關警報名稱、狀態、通知方式和通知頻率的資訊。您也可以在此頁面新增、編輯、移除、啟用或停用警報。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

命令按鈕

- 新增

  顯示「新增警報」對話方塊，可讓您新增警報。

- 編輯

  顯示「編輯警報」對話方塊，讓您編輯選定的警報。

- 刪除

  刪除選取的警報。

- 啟用

  啟用所選警報以發送通知。

- 停用

  當您想要暫時停止傳送通知時，停用所選的警示。

- 測試

  新增或編輯後，測試選定的警報以驗證其組態。

- 已解決和已過時事件的警示

  允許您啟用或停用事件狀態變為「已解決」或「已過時」時發送的提醒。這有助於使用者避免接收不必要的通知。

清單檢視

清單檢視以表格形式顯示已建立的警報資訊。您可以使用欄篩選器自訂顯示的資料。您也可以選擇某個警報，在詳細資訊區域檢視更多相關資訊。

- 狀態

  指定警報是否啟用（）或停用（）。

- 警報

  顯示警報名稱。

- 說明

  顯示警報的執行摘要。

- 通知方式

  顯示為警報選擇的通知方式。您可以透過電子郵件或 SNMP 陷阱通知使用者。

- 通知頻率

  指定管理伺服器持續發送通知的頻率（以分鐘為單位），直到事件被確認、解決或移至過時狀態。

詳細資訊區域

詳細資訊區域提供有關所選警報的更多資訊。

- 警報名稱

  顯示警報名稱。

- 警報執行摘要

  顯示警報的執行摘要。

- 事件

  顯示您希望觸發警報的事件。

- 資源

  顯示要觸發警報的資源。

- 包含

  顯示要觸發警報的資源群組。

- 不包括

  顯示您不想觸發警報的資源群組。

- 通知方式

  顯示警報的通知方式。

- 通知頻率

  顯示管理伺服器持續傳送警報通知的頻率，直到事件被確認、解決或移至過時狀態為止。

- 指令碼名稱

  顯示與所選警報關聯的指令碼名稱。該指令碼在產生警報時執行。

- 郵件收件者

  顯示收到警報通知的使用者的電子郵件地址。

了解 **Active IQ Unified Manager** 中的「新增警報」對話方塊

您可以建立警報，以便在發生特定事件時收到通知，從而快速解決問題，最大限度地減少對環境的影響。您可以為單一資源或一組資源建立警報，也可以為特定嚴重性類別的事件建立警報。此外，您也可以指定警報的通知方式和頻率。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

Name

您可以在此指定警報的名稱和執行摘要：

- 警報名稱

  允許您指定警報名稱。

- 警報執行摘要

  允許您為警報指定執行摘要。

資源

在此區域，您可以選擇單一資源，或根據動態規則對資源進行分組，以觸發警報。動態規則 是指根據您指定的字串篩選出的資源集合。您可以從下拉清單中選擇資源類型來搜尋資源，也可以指定確切的資源名稱來顯示特定資源。

如果您從任何儲存設備物件詳細資料頁面建立警報，則儲存設備物件會自動包含在警報中。

- 包括

  可讓您包含要觸發警報的資源。您可以指定字串來將符合該字串的資源分組，並選取要包含在警報中的此群組。例如，您可以將名稱包含 "abc" 字串的所有磁碟區分組。

- 排除

  可讓您排除不想觸發警報的資源。例如，您可以排除名稱包含 "xyz" 字串的所有磁碟區。

只有當您選擇特定資源類型的所有資源時，才會顯示「排除」標籤：例如，<<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>。

如果資源同時符合您指定的包含規則和排除規則，則排除規則優先於包含規則，並且不會為該事件產生警報。

事件

在此區域，您可以選擇要為其建立警報的事件。您可以根據特定嚴重程度或一組事件建立警報。

若要選擇多個事件，您應該在進行選擇時按住 Ctrl 鍵。

- 事件嚴重程度

  允許您根據嚴重性類別選擇事件，該類別可以是「嚴重」、「錯誤」或「警告」。

- 事件名稱包含

  允許您選擇名稱包含指定字元的事件。

動作

在此區域，您可以指定觸發警報時要通知的使用者。您也可以指定通知方式和通知頻率。

- 通知這些使用者

  允許您指定接收通知的使用者的電子郵件地址或使用者名稱。

  如果您修改為使用者指定的電子郵件地址，並重新開啟警報以進行編輯，則「名稱」欄位會顯示為空白，因為修改後的電子郵件地址不再對應至先前選取的使用者。此外，如果您從「使用者」頁面修改了所選使用者的電子郵件地址，則修改後的電子郵件地址不會為所選使用者更新。

- 通知頻率

  可讓您指定管理伺服器傳送通知的頻率，直到事件獲得確認、解決或移至過時狀態為止。

  您可以選擇以下通知方式：

  - 僅通知一次
  - 按指定頻率通知
  - 在指定的時間範圍內，以指定的頻率發出通知

- 發出 **SNMP** 陷阱

  勾選此方塊可指定是否應將 SNMP 陷阱傳送至全域設定的 SNMP 主機。

- 執行指令碼

  可讓您將自訂指令碼新增至警報。產生警報時會執行此指令碼。

> 如果您在使用者介面中看不到此功能，則是因為您的系統管理員已停用該功能。如有需要，您可以從 儲存設備管理 > 功能設定 啟用此功能。

命令按鈕

- 儲存

  建立警示並關閉對話方塊。

- 取消

  放棄變更並關閉對話方塊。

在 **Active IQ Unified Manager** 中編輯警示屬性

您可以編輯警報屬性，例如警報關聯的資源、事件、指令碼和通知選項。

Name

您可以在此處編輯警報的名稱和執行摘要。

- 警報名稱

  可讓您編輯警報名稱。

- 警報執行摘要

  允許您為警報指定執行摘要。

- 警報狀態

  允許您啟用或停用警報。

資源

在此區域，您可以選擇單一資源，或根據動態規則對資源進行分組，以觸發警報。您可以從下拉清單中選擇資源類型來搜尋資源，也可以指定確切的資源名稱來顯示特定資源。

- 包括

  可讓您包含要觸發警報的資源。您可以指定字串來將符合該字串的資源分組，並選取此群組以包含在警報中。例如，您可以將名稱包含 “vol0” 字串的所有 Volume 分組。

- 排除

  允許您排除不想觸發警報的資源。例如，您可以排除名稱包含 “xyz” 字串的所有 Volume。

  只有當您選擇特定資源類型的所有資源時，才會顯示「排除」標籤——例如，<<All Volumes>> 或 <<All Volumes whose name contains 'xyz'>>。

事件

在此區域，您可以選擇要觸發警報的事件。您可以根據特定嚴重程度或一組事件觸發警報。

- 事件嚴重程度

允許您根據嚴重性類別選擇事件，該類別可以是「嚴重」、「錯誤」或「警告」。

- 事件名稱包含

  允許您選擇名稱包含指定字元的事件。

動作

您可以在此指定通知方式和通知頻率。

- 通知這些使用者

  您可以編輯電子郵件地址或使用者名稱，或指定新的電子郵件地址或使用者名稱來接收通知。

- 通知頻率

  您可以編輯管理伺服器發送通知的頻率，直到事件被確認、解決或移至過時狀態。

  您可以選擇以下通知方式：

  - 僅通知一次
  - 按指定頻率通知
  - 在指定的時間範圍內，以指定的頻率發出通知

- 發出 **SNMP** 陷阱

  允許您指定是否應將 SNMP 陷阱傳送至全域設定的 SNMP 主機。

- 執行指令碼

  可讓您將指令碼與警報建立關聯。產生警報時，即會執行此指令碼。

命令按鈕

- 儲存

  儲存變更並關閉對話方塊。

- 取消

  放棄變更並關閉對話方塊。

管理指令碼

在 **Active IQ Unified Manager** 中管理指令碼

您可以使用指令碼自動修改或更新 Unified Manager 中的多個儲存設備物件。該指令碼與警報關聯。當事件觸發警報時，指令碼將會執行。您可以上傳自訂指令碼，並在產生警報時測試其執行情況。

預設情況下，上傳指令碼到 Unified Manager 並執行指令碼的功能已啟用。如果出於安全性原因，您的組織不希望允許此功能，您可以從 儲存設備管理 > 功能設定 中停用此功能。

相關資訊

"啟用和停用指令碼上傳功能"

Active IQ Unified Manager 中的指令碼如何與警報協同運作

您可以將警報與指令碼建立關聯，以便在 Unified Manager 中發生事件並觸發警報時執行該指令碼。您可以使用這些指令碼來解決儲存設備物件的問題，或識別哪些儲存設備物件正在產生事件。

當 Unified Manager 中某個事件產生警報時，系統會傳送警報郵件給指定的收件者。如果您已將警報與指令碼關聯，則會執行該指令碼。您可以從警報郵件中取得傳遞給指令碼的參數詳細資料。

如果您建立了自訂指令碼並將其與特定事件類型的警報建立關聯，則會根據您針對該事件類型的自訂指令碼採取行動，並且預設情況下，修復 行動在「管理行動」頁面或 Unified Manager 儀表板上無法使用。

該指令碼使用以下參數執行：

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

您可以在指令碼中使用這些參數，並收集相關的事件資訊或修改儲存設備物件。

從指令碼中取得參數的範例

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

當產生警報時，將執行此指令碼並顯示以下輸出：

```
-`eventID : 290`
-`eventSourceID : 4138`
```

在 **Active IQ Unified Manager** 中新增指令碼

您可以在 Unified Manager 中新增指令碼，並將這些指令碼與警報關聯。當產生警報時，這些指令碼會自動執行，使您能夠取得有關觸發事件的儲存設備物件的資訊。

開始之前

- 您必須已經建立並儲存要新增至 Unified Manager 伺服器的指令碼。
- 指令碼支援的檔案格式有 Perl、Shell、PowerShell、Python 和 `.bat` 檔案。

安裝 **Unified Manager** 的平台	支援的語言
VMware	Perl 和 Shell 指令碼
Linux	Perl、Python 和 Shell 指令碼
Windows	PowerShell、Perl、Python 和 .bat 指令碼

  - 對於 Perl 指令碼，必須在 Unified Manager 伺服器上安裝 Perl。對於 VMware 安裝，預設會安裝 Perl 5，且指令碼僅支援 Perl 5 支援的功能。如果 Perl 是在 Unified Manager 之後才安裝，則必須重新啟動 Unified Manager 伺服器。
  - 對於 PowerShell 指令碼，必須在 Windows 伺服器上設定適當的 PowerShell 執行原則，以便指令碼能夠執行。

> 如果您的指令碼會建立記錄檔來追蹤警報指令碼的進度，您必須確保記錄檔不會建立在 Unified Manager 安裝資料夾內的任何位置。

- 您必須擁有應用程式系統管理員或儲存系統管理員角色。

您可以上傳自訂指令碼並收集有關警報的事件詳細資訊。

> 如果您在使用者介面中看不到此功能，則是因為您的系統管理員已停用該功能。如有需要，您可以從 儲存設備管理 > 功能設定 啟用此功能。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 指令碼。
2. 在「指令碼」頁面中，按一下「新增」。
3. 在 新增指令碼 對話方塊中，按一下 瀏覽 選擇您的指令碼檔案。
4. 請輸入所選指令碼的執行摘要。
5. 點擊 **Add** 。

相關資訊

"啟用和停用指令碼上傳功能"

在 **Active IQ Unified Manager** 中刪除指令碼

當指令碼不再需要或無效時，您可以從 Unified Manager 中刪除該指令碼。

開始之前

- 您必須擁有應用程式系統管理員或儲存系統管理員角色。
- 該指令碼不得與警報關聯。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 指令碼。
2. 在 指令碼 頁面中，選取您要刪除的指令碼，然後按一下 刪除。
3. 在「警告」對話方塊中，按一下「是」確認刪除。

在 **Active IQ Unified Manager** 中執行測試指令碼

當儲存設備物件產生警報時，您可以驗證指令碼是否正確執行。

開始之前

- 您必須擁有應用程式系統管理員或儲存系統管理員角色。
- 您必須將指令碼以支援的檔案格式上傳至 Unified Manager。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 指令碼。
2. 在 指令碼 頁面中，新增您的測試指令碼。
3. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
4. 在「警報設定」頁面中，執行下列行動之一：

若要.....	這樣做.....
新增提醒	a. 點擊 **Add** 。 b. 在「行動」部分，將警報與您的測試指令碼建立關聯。
編輯提醒	a. 選取警報，然後點選 編輯。 b. 在「行動」部分，將警報與您的測試指令碼建立關聯。

5. 按一下 **Save** 。
6. 在 警報設定 頁面中，選擇您新增或修改的警報，然後按一下 測試。

   指令碼以「-test」參數執行，並將通知警報傳送至建立警報時指定的電子郵件地址。

瞭解受支援的 **Active IQ Unified Manager CLI** 指令

身為儲存管理員，您可以使用 CLI 命令對儲存設備物件執行查詢；例如，對叢集、彙總、Volume、qtree 和 LUN 執行查詢。您可以使用 CLI 命令查詢 Unified Manager 內部資料庫和 ONTAP 資料庫。您也可以在指令碼中使用 CLI 命令，這些指令碼會在作業開始或結束時執行，或在觸發警示時執行。

所有命令之前都必須加上命令 `um cli login`，以及用於驗證的有效使用者名稱和密碼。

若要執行 *um run* 命令，請確定您的帳戶具有 *console* 應用程式存取權。

CLI 指令	說明	輸出
`um cli login -u <username> [-p <password>]`	登入命令列介面（CLI）。基於安全性考量，您應該只在「-u」選項之後輸入使用者名稱。以這種方式使用時，系統會提示您輸入密碼，且密碼不會記錄在歷史記錄或程序表中。工作階段會在登入後三小時過期，之後使用者必須重新登入。	顯示相應的訊息。
`um cli logout`	登出 CLI。	顯示相應的訊息。
`um help`	顯示所有第一層級子命令。	顯示所有第一層級子命令。
`um run cmd [ -t <timeout> ] <cluster> <command>`	在單一或多個主機上執行命令的最簡單方法。主要用於警示指令碼，以取得 ONTAP 的相關資訊或執行相關操作。選用的逾時引數會設定命令在用戶端完成的最大時間限制（以秒為單位）。預設值為 0（無限期等待）。	從 ONTAP 接收到的。
`um run query <sql command>`	執行 SQL 查詢。僅允許執行從資料庫讀取的查詢。不支援任何更新、插入或刪除作業。	結果以表格顯示。如果傳回空集，或有任何語法錯誤或無效請求，則會顯示對應的錯誤訊息。
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	將資料來源新增至代管儲存設備系統清單中。資料來源描述如何與儲存設備系統建立連線。新增資料來源時，必須指定選項 -u（使用者名稱）和 -P（密碼）。選項 -t（協定）指定用於與叢集通訊的協定（http 或 https）。如果未指定協定，則會嘗試使用兩種協定。選項 -p（連接埠）指定用於與叢集通訊的連接埠。如果未指定連接埠，則會嘗試使用相應協定的預設值。此命令只能由儲存管理員執行。	提示使用者接受憑證並列印相應的訊息。
`um datasource list [ <datasource-id>]`	顯示代管儲存設備系統的資料來源。	以表格形式顯示以下值： `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message`。

CLI 指令	說明	輸出
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	修改一個或多個資料來源選項。只能由儲存管理員執行。	顯示相應的訊息。
`um datasource remove <datasource-id>`	從 Unified Manager 中移除資料來源（叢集）。	顯示相應的訊息。
`um option list [ <option> .. ]`	列出所有可以使用 set 命令設定的選項。	以表格形式顯示以下值：`Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	設定一個或多個選項。此命令只能由儲存管理員執行。	顯示相應的訊息。
`um version`	顯示 Unified Manager 軟體版本。	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	列出按指定物件篩選後的 LUN。-q 適用於所有命令，表示不顯示標題。ObjectType 可以是 lun、qtree、cluster、Volume、配額或 svm。 例如： **`um lun list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內的所有 LUN。	以表格形式顯示以下值：`ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	列出按指定物件篩選後的儲存設備虛擬機器。ObjectType 可以是 lun、qtree、cluster、Volume、配額或 svm。 例如： **`um svm list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內所有的儲存設備虛擬機器。	以表格形式顯示以下值：`Name and Cluster ID.`

CLI 指令	說明	輸出
`um qtree list [-q] [ -ObjectType <object-id>]`	列出按指定物件篩選後的 qtree。-q 適用於所有命令，表示不顯示標題。ObjectType 可以是 lun、qtree、cluster、Volume、配額或 svm。 例如： **`um qtree list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內的所有 qtree。	以表格形式顯示以下值：`Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的磁碟。ObjectType 可以是磁碟、aggr、節點或叢集。 例如： **`um disk list -cluster 1`** 在此範例中，"-cluster" 是 objectType，而 "1" 是 objectId。此命令會列出 ID 為 1 的叢集內的所有磁碟。	以表格形式顯示以下值 `ObjectType and object-id。`
`um cluster list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的叢集。ObjectType 可以是磁碟、aggr、節點、cluster、lun、qtree、Volume、配額或 svm。 例如： **`um cluster list -aggr 1`** 在這個範例中，「-aggr」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的彙總所屬的叢集。	以表格形式顯示以下值：`Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key。`

CLI 指令	說明	輸出
`um cluster node list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的叢集節點。ObjectType 可以是磁碟、aggr、節點或叢集。 例如： **`um cluster node list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內的所有節點。	以表格形式顯示以下值 `Name and Cluster ID`。
`um volume list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的 Volume。ObjectType 可以是 lun、qtree、cluster、Volume、配額、svm 或彙總。 例如： **`um volume list -cluster 1`** 在此範例中，"-cluster" 是 objectType，而 "1" 是 objectId。此命令會列出 ID 為 1 的叢集內的所有 Volume。	以表格形式顯示以下值 `Volume ID and Volume Name`。
`um quota user list [-q] [-ObjectType <object-id>]`	列出按指定物件篩選後的配額使用者。ObjectType 可以是 qtree、cluster、Volume、配額或 svm。 例如： **`um quota user list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內所有配額使用者。	以表格形式顯示以下值 `ID, Name, SID and Email`。

CLI 指令	說明	輸出
`um aggr list [-q] [-ObjectType <object-id>]`	列出依指定物件篩選後的 Aggregate。ObjectType 可以是磁碟、aggr、節點、cluster 或 Volume。 例如： **`um aggr list -cluster 1`** 在此範例中，「-cluster」是 objectType，而「1」是 objectId。此命令會列出 ID 為 1 的叢集內的所有 Aggregate。	以表格形式顯示以下值 `Aggr ID, and Aggr Name`。
`um event ack <event-ids>`	確認一個或多個事件。	顯示相應的訊息。
`um event resolve <event-ids>`	解決一個或多個事件。	顯示相應的訊息。
`um event assign -u <username> <event-id>`	將事件指派給使用者。	顯示相應的訊息。
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	列出系統或使用者產生的事件。根據來源、狀態和 ID 篩選事件。	以表格格式顯示下列值 `Source, Source type, Name, Severity, State, User and Timestamp`。
`um backup restore -f <backup_file_path_and_name>`	使用 .7z 檔案還原 MySQL 資料庫備份。	顯示相應的訊息。

指令碼視窗和對話方塊的說明

了解 **Active IQ Unified Manager** 中的「指令碼」頁面

「指令碼」頁面可讓您將自訂指令碼新增至 Unified Manager。您可以將這些指令碼與警報建立關聯，以啟用儲存設備物件的自動重新組態。

指令碼頁面可讓您從 Unified Manager 新增或刪除指令碼。

命令按鈕

- 新增

  顯示「新增指令碼」對話方塊，讓您可以新增指令碼。

- 刪除

  刪除選定的指令碼。

清單檢視

清單檢視以表格形式顯示您新增至 Unified Manager 的指令碼。

- 名稱

  顯示指令碼名稱。

- 說明

  顯示指令碼的執行摘要。

在 **Active IQ Unified Manager** 中新增指令碼對話方塊

「新增指令碼」對話方塊可讓您為 Unified Manager 新增指令碼。您可以使用指令碼設定警報，以便自動解決為儲存設備物件產生的事件。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

- 選擇指令碼檔案

  可讓您為警報選擇指令碼。

- 說明

  允許您為指令碼指定執行摘要。

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。